IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

In re: Equifax, Inc. Customer Data Security Breach Litigation	)	MDL Docket No. 2800 Case No.: 1:17-md-2800-TWT
	)	**CONSUMER ACTIONS**

CONSOLIDATED CLASS ACTION COMPLAINT FOR SMALL BUSINESS CLAIMS

Amy E. Keller
DiCELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602

Kenneth S. Canfield
DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree Street, N.E. Suite 1900
Atlanta, Georgia 30309

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112

Consumer Plaintiffs' Co-Lead Counsel
Other Counsel Identified on Signature Pages

The plaintiffs identified below (collectively, "Business Plaintiffs"), individually and on behalf of the Classes defined below of similarly situated business entities, allege the following against Defendants Equifax Inc., Equifax Information Services LLC ("EIS"), and Equifax Consumer Services LLC ("ECS") (collectively, "Equifax" or "Defendants"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Equifax plays a central role in the modern American economy, collecting and selling vast amounts of data about the most important details of consumers' financial lives. That data—names, birthdates, Social Security numbers, credit card information, drivers' license numbers, and more—contains the keys that unlock a consumer's identity and is relied upon by third parties to make major financial decisions affecting almost all Americans. Equifax understood it had an enormous responsibility to protect the data it collected and assured the public that: "At Equifax, the security of our customers' information is paramount." But, as its former CEO has acknowledged, Equifax has not lived up to that responsibility or fulfilled its public assurances to protect Americans' confidential information.

2. On September 7, 2017, Equifax announced that it was subject to one of the largest data breaches in our nation's history. Taking advantage of glaring weaknesses and vulnerabilities in the company's data security systems, hackers stole the personal and financial information of nearly 150 million Americans from mid-May through the end of July, 2017. During that entire two and one-half month period, Equifax failed to detect the hackers' presence, notice the massive amounts of data that were being exfiltrated from its databases, or take any steps to investigate the numerous other red flags that should have warned the company about what was happening.

3. Equifax has attributed the breach to a low-level employee's failure to install a necessary software patch. While that employee's negligence may have created the door through which the hackers first entered, the breach was in fact the inevitable result of Equifax's systemic incompetence and a longstanding, lackluster approach to data security that permeated the company's culture from the top down. Indeed, Equifax's cavalier attitude about data security persisted despite warnings by outside cybersecurity experts, the occurrence of other data breaches at Equifax, and numerous high-profile data breaches at other major American corporations, all of which should have alerted Equifax of the need to revamp and enhance its woefully inadequate data security practices.

4. The severity of this breach is unprecedented, affecting almost half of the American population. Nearly all of the victims had no prior relationship with Equifax, and there is no mechanism to opt-out of Equifax's collection and sale of this data. The hackers obtained at least 146.6 million names, 146.6 million dates of birth, 145.5 million Social Security numbers, 99 million addresses, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 tax identification numbers. Using this information, identity thieves can create fake identities, fraudulently obtain loans and tax refunds, and destroy a consumer's credit-worthiness—the very thing Equifax exists to assess and report. And because Social Security numbers do not expire and are almost impossible to change, thieves will be able to do so for years to come. As one knowledgeable analyst noted soon after the breach was announced: "On a scale of 1 to 10 in terms of risk to consumers, this is a 10."

5. Since the Equifax breach occurred, small businesses across the United States have been directly and negatively impacted because of the breach, incurring costs to mitigate the risk, such as buying credit monitoring products or spending $100 for a business credit report that would have been unnecessary but for the Equifax data breach. Equifax's negligence and the resulting breach have jeopardized that credit, and small businesses around the country are at risk of losing their access

to credit, having to pay more for credit (for example, through higher interest rates), losing their collateral, and struggling to maintain their operations. They remain subject to a pervasive, substantial, and imminent risk of fraud and negative credit consequences flowing from the unauthorized dissemination of their owners' Personal Information.

6. Financial advisors, experts, and even the media are advising such businesses to procure business credit monitoring and other credit protection products, which are sold by Equifax and other entities. Although Equifax has been urged repeatedly to provide these products to small businesses for free after the breach, it has refused to do so and instead continues to profit from the credit concerns that it caused.

7. As further described herein, Business Plaintiffs assert claims for themselves, and on behalf of all similarly situated businesses in the United States, for Equifax's negligence, negligence *per se*, and for violations of state statute. Business Plaintiffs seek all available monetary relief, including damages and restitution, and equitable relief, including an injunction to halt Equifax's unlawful conduct.

JURISDICTION AND VENUE

8. This Consolidated Complaint and is intended to serve as a superseding complaint as to all previous complaints centralized in this multidistrict litigation that were filed on behalf of non-financial institution business entities, and to serve as the operative pleading on behalf of such entities. As set forth herein, this Court has general jurisdiction over Equifax and original jurisdiction over Business Plaintiffs' claims.

9. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, and Equifax is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

10. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Equifax's principal place of business is located in this District and substantial parts of the events or omissions giving rise to the claims occurred in the District. Venue is also proper in the Atlanta Division because Equifax is located here and the causes of action arose here.

NAMED PLAINTIFFS

11. The below Business Plaintiffs appear on behalf of themselves and those similarly situated. Equifax, through its actions described herein, has caused them present, immediate, imminent, and continuing increased risk of harm.

CALIFORNIA

12. Business Plaintiff Sharps Investment Enterprises, LLC, is a limited liability company existing under the laws of the State of California. Sharps Investment Enterprises, LLC, relies in part on credit to operate. Sharps Investment Enterprises, LLC, relies on the personal credit of Joshua Sharps, the individual whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only Joshua Sharps' personal credit, but also the creditworthiness and continued operations of Sharps Investment Enterprises, LLC. Sharps Investment Enterprises, LLC, has reasonably incurred costs (in the form of a business credit report and devotion of resources to monitoring its financial accounts) based on the substantial risk of harm from the breach.

DELAWARE

13. Business Plaintiff The Mello Group, Inc., is a corporation and a small business existing under the laws of the State of Delaware. The Mello Group, Inc.,

relies in part on credit to operate. The Mello Group, Inc., relies on the personal credit of Chris Williams, an individual whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only his personal credit, but also the creditworthiness and continued operations of The Mello Group, Inc. The Mello Group, Inc., has reasonably incurred costs (in the form of a business credit report and devotion of resources to monitoring its financial accounts) based on the substantial risk of harm from the breach.

FLORIDA

14. Business Plaintiff Pierce N Tell of Sarasota, LLC, is a limited liability company existing under the laws of the State of Florida. Pierce N Tell of Sarasota, LLC, relies in part on credit to operate. Pierce N Tell of Sarasota, LLC, relies on the personal credit of Oshik Perez, an individual whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only his personal credit, but also the creditworthiness and continued operations of Pierce N Tell of Sarasota, LLC. Pierce N Tell of Sarasota, LLC, has reasonably incurred costs (in the form of a business credit report and devotion of resources to monitoring its financial accounts) based on the substantial risk of harm from the breach.

GEORGIA

15. Business Plaintiff Forest Express Properties, LLC, is a limited liability company existing under the laws of the State of Georgia. Forest Express Properties, LLC, relies in part on credit to operate. Forest Express Properties, LLC, relies on the personal credit of Akbar Ali and Poonam Ali, individuals whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only their personal credit, but also the creditworthiness and continued operations of Forest Express Properties, LLC. Forest Express Properties, LLC, has reasonably incurred costs (in the form of a business credit report and devotion of resources to monitoring its financial accounts) based on the substantial risk of harm from the breach.

16. Business Plaintiff St. Luc Holdings (SLH), LLC f/k/a Just Rev, LLC ("Just Rev"), is a limited liability company existing under the laws of the State of Georgia. Just Rev, LLC, relies in part on credit to operate. Just Rev, LLC, relies on the personal credit of Reevney St. Luc, an individual whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only his personal credit, but also the creditworthiness and continued operations of Just Rev, LLC. Just Rev, LLC, has reasonably incurred costs (in the form of a business credit report and devotion of

resources to monitoring its financial accounts) based on the substantial risk of harm from the breach.

17. Business Plaintiff Martin's Auto Repair, is a partnership and a small business existing under the laws of the State of Georgia. Martin's Auto Repair relies in part on credit to operate. Martin's Auto Repair relies on the personal credit of Teresa Sue Martin and William Marvin Martin, Jr., individuals whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only their personal credit, but also the creditworthiness and continued operations of Martin's Auto Repair. Martin's Auto Repair, has reasonably incurred costs (in the form of a business credit report and devotion of resources to monitoring its financial accounts) based on the substantial risk of harm from the breach.

18. Business Plaintiff Rafco, LLC, is a limited liability company existing under the laws of the State of Georgia. Rafco, LLC, relies in part on credit to operate. Rafco, LLC, relies on the personal credit of Rahul Faruqi, an individual whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only his personal credit, but also the creditworthiness and continued operations of Rafco, LLC. Rafco, LLC, has reasonably incurred costs (in the form of a business credit report and devotion

of resources to monitoring its financial accounts) based on the substantial risk of harm from the breach.

MISSISSIPPI

19. Business Plaintiff Kademi, LLC, is a limited liability company existing under the laws of the State of Mississippi. Kademi, LLC, relies in part on credit to operate. Kademi, LLC, relies on the personal credit score of Dawn Lea Chalmers and Kimberly Kilpatrick, individuals whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only her personal credit, but also the creditworthiness and continued operations of Kademi, LLC. Kademi, LLC, has reasonably incurred costs (in the form of a business credit report and devotion of resources to monitoring its financial accounts) based on the substantial risk of harm from the breach.

OHIO

20. Business Plaintiff Champs Sports Bar & Grill Co., d/b/a TJ's on the Avenue, is a for-profit corporation and small business existing under the laws of the State of Ohio. Champs Sports Bar & Grill Co. relies in part on credit to operate. Champs Sports Bar & Grill Co. relies on the personal credit of Craig Pulling, an individual whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only his

personal credit, but also the creditworthiness and continued operations of Champs Sports Bar & Grill Co. In addition, as a result of the breach, Craig Pulling spent time and effort on behalf of Plaintiff Champs Sports Bar & Grill Co. monitoring financial accounts and searching for fraudulent activity, based on the substantial risk of harm from the breach.

TEXAS

21. Business Plaintiff Coastal Communications, LLC, is a limited liability company existing under the laws of the State of Texas. Coastal Communications, LLC, relies in part on credit to operate. Coastal Communications, LLC, relies on the personal credit score of Jeff Newkirk, an individual whose Personal Information was compromised in the Equifax breach, to obtain and maintain its own credit. The breach has thus jeopardized not only his personal credit, but also the creditworthiness and continued operations of Coastal Communications, LLC. Coastal Communications, LLC, has reasonably incurred costs (in the form of a business credit report and devotion of resources to monitoring its financial accounts) based on the substantial risk of harm from the breach.

DEFENDANTS AND THEIR RELEVANT CORPORATE STRUCTURE

22. Defendant Equifax Inc. is a Georgia corporation, with its principal place of business in Atlanta, Georgia. Equifax is subject to the jurisdiction of this

Court and may be served with process through its registered agent, Shawn Baldwin, 1550 Peachtree Street, N.W., Atlanta, Fulton County, Georgia. Equifax Inc. is the parent company of Defendants Equifax Information Services LLC and Equifax Consumer Services LLC.

23. Defendant Equifax Information Services LLC is a Georgia limited liability company, with its principal place of business in Atlanta, Georgia. Equifax Information Services LLC is subject to the jurisdiction of this Court and may be served with process through its registered agent, Shawn Baldwin, 1550 Peachtree Street, N.W., Atlanta, Fulton County, Georgia.

24. Defendant Equifax Consumer Services LLC is a Georgia limited liability company, with its principal place of business in Atlanta, Georgia. Equifax Consumer Services LLC is subject to the jurisdiction of this Court and may be served with process through its registered agent, Shawn Baldwin, 1550 Peachtree Street, N.W., Atlanta, Fulton County, Georgia.

25. Defendants operate together as a unified consumer reporting agency ("CRA") to prepare and furnish consumer reports for credit and other purposes. All three Defendants are both "consumer reporting agencies" and "nationwide reporting agencies" as defined by the Fair Credit Reporting Act ("FCRA").

26. Throughout the events at issue here, Defendants have operated as one entity and CRA. As it pertains to consumer reporting, Equifax Inc. has used EIS and ECS as dependent and integrated divisions rather than as separate legal entities. The business operations are fully coordinated and shared. Resources are cross-applied without full and complete cost and profit centers. Management decisions at EIS and ECS are made by and through management of Equifax Inc. The management of Equifax Inc. was and is directly involved in the events at issue in this litigation, including Equifax's cybersecurity, the breach itself, and Defendants' response to the breach.

27. To remain separate and distinct for the purposes of liability in this action, Defendants must operate as separate and distinct legal and operational entities. Here, for the matters and functions alleged and relevant herein, EIS and ECS were merely alter egos of Equifax Inc. For purposes of how consumer data was handled, warehoused, used and sold, the corporate distinctions were disregarded in practice. EIS and ECS were mere instrumentalities for the transaction of the corporate consumer credit business. Defendants shared full unity of interest and ownership such that the separate personalities of the corporation and subsidiaries no longer existed.

28. Further, recognition of the technical corporate formalities in this case would cause irremediable injustice and permit Equifax Inc.—the entity whose management caused and permitted the events alleged herein—to defeat justice and to evade responsibility. *See Derbyshire v. United Builders Supplies, Inc.*, 194 Ga. App. 840, 844 (1990).

29. Accordingly, for all purposes hereafter, when Business Plaintiffs allege "Equifax" as the actor or responsible party, they are alleging the participation and responsibility of all three Defendants collectively.

STATEMENT OF FACTS

The Importance of Consumer Credit in the U.S. Economy

30. A consumer credit system allows consumers to borrow money or incur debt, and to defer repayment of that money over time. Access to credit enables consumers to buy goods or assets without having to pay for them in cash at the time of purchase.[1] Nearly all Americans rely on credit to make everyday purchases using credit cards, obtain student loans and further education, gain approval for items like

[1] M. Greg Braswell and Elizabeth Chernow, *Consumer Credit Law & Practice in the U.S.*, THE U.S. FEDERAL TRADE COMMISSION at 1, https://www.ftc.gov/sites/default/files/attachments/training-materials/law_practice.pdf (last accessed May 11, 2018) ("FTC, *Consumer Credit Law & Practice in the U.S.*").

cellular phones and Internet access, and to make major life purchases such as automobiles and homes.

31. In order for this system of credit to be efficient and effective, a system of evaluating the credit of consumers is required. The earliest American systems of credit evaluation were retailers relying on personal reputation and standing in the community to determine creditworthiness. U.S. credit reporting agencies started as associations of retailers who shared their customers' credit information with each other including those deemed as credit risks.[2]

32. As the nation grew after World War II, and banks and finance companies took over from retailers as the primary source of consumer credit, a more quantitative and objective system of credit rating emerged. The development of computers, which could store and process large amounts of data, enabled the CRAs to efficiently collect and provide credit information to consumer lenders on a national basis.[3]

33. Today, creditors such as banks and mortgage companies loan money to consumers, track the consumers' payment history on the loan, and then provide that information to one or more CRAs. The CRAs track all of the payment history they

[2] *Id*.
[3] *Id*. at 2.

receive relating to a single consumer and compile that information as part of a consumer's credit reporting "file."[4]

34. A consumer's credit reporting file contains identifying information such as the consumer's name, date of birth, address, and Social Security Number (SSN), as well as payment information on past credit accounts, including the name of the lender, the original amount of the loan, the type of the loan, and how much money the consumer still owes on that loan. A consumer file also contains details on the consumer's payment history on past credit accounts—which helps potential lenders estimate how likely the consumer is to pay back the full amount of a loan on time—and information in the public record which might affect the consumer's ability to pay back a loan, such as recent bankruptcy filings, pending lawsuits, or information relating to tax liabilities.[5]

35. Because consumers have little or no control over the information that CRAs gather and store, the accuracy and security of the information they compile is at the heart of a fair and accurate credit reporting system. Information that is inaccurate can lead to uninformed credit decisions, and information that is unsecure

[4] *Id*.

[5] *Id*. at 1.

can lead to identify theft, fraud, and widespread distrust of CRAs—with systemic consequences for the entire national economy.

Equifax Compiles Massive Amounts of Consumer Information

36. Equifax first did business in 1899 as Retail Credit Company. At that time, most of its operation was dedicated to gathering information for insurance companies, including information on people's finances, health, moral beliefs, vehicle use and other factors that insurance companies used when quoting for life, car, and health insurance policies. Critics asserted that Retail Credit Company "reinforced preexisting social inequalities and rationalized 'fair' discrimination as a cornerstone of the capitalist economy. For women and poor African Americans, for example, a Retail Credit Company report did not open doors to financial security. It just recorded how society already saw you: as a bad risk."[6]

37. By the mid-1960s, Retail Credit Company had nearly 300 branch offices and maintained files on millions of Americans. The company sold stock to the public for the first time in 1965. While many CRAs at the time gathered only names, birth dates, address, and payment history for consumers, "Retail Credit

[6] Rachel Bunker, *The Equifax Way*, JACOBIN MAGAZINE (Sept. 18, 2017), https://www.jacobinmag.com/2017/09/equifax-retail-credit-company-discrimination-loans (last accessed May 11, 2018).

Company, which specialized in insurance reporting, gathered far more information on consumers."[7]

38. An article published in the New Republic in 1966 documented how Retail Credit Company "inspectors" and investigators "collected the most intimate details of an individual's life, including information about their race and sexual habits, their church attendance, their home environment, and whether or not they were experiencing marital discord."[8] The article warned that the information "could have originated from potentially unreliable neighbors and acquaintances" and that "[i]f damaging or just plain wrong information had managed to creep into a person's file, they were at the mercy of the credit bureau, since it was nearly impossible to see these confidential consumer reports."[9]

39. In March 1970, Alan Westin, a Columbia University professor, wrote an article critical of Retail Credit Company in *The New York Times* after reviewing a sample of the company's files and discovering that they included "facts, statistics, inaccuracies, and rumors" about virtually every phase of an individual's life,

[7] *Id.*

[8] *Id.*

[9] *Id.*

including "marital troubles, jobs, school history, childhood, sex life and political activities."

40. That same month, as Retail Credit Company moved towards digitizing its records, Westin testified before Congress about how widespread inaccuracies could result in consumers being unfairly denied credit. In response, Congress enacted the FCRA in October 1970 "to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies."

41. To fend off negative publicity and help improve its image, in late 1975 Retail Credit Company changed its name to "Equifax Inc." Over the next two decades, Equifax expanded rapidly by acquiring many of its rivals and increasing its data collection capacity. By the late 1990s, industry-consolidation resulted in three major CRAs controlling the market: Equifax, Experian, and TransUnion.

42. Equifax's business model involves aggregating data relating to consumers from various sources, compiling that data in a usable format known as a credit report, and selling access to those reports to lenders interested in making credit decisions, financial companies, employers, and other entities that use those reports to make decisions about individuals in a range of areas. Because the extension of

credit relies on access to consumers' credit files, the CRAs have been referred to as the "linchpins" of the U.S. financial system.[10]

43. Equifax also sells information directly to consumers, including access to their own credit file (known as a "consumer disclosure"). In 2001, Equifax partnered with the Fair Isaac Corporation ("FICO") to allow consumers to purchase their three-digit FICO credit scores, which are numerical values generated to represent the "creditworthiness" of a consumer. Equifax sells a number of credit-related products tailored to consumers and businesses interested in monitoring their credit. Today, Equifax's consumer business alone generates $400 million in annual sales.

44. In addition to providing services to individual consumers, Equifax supplies identity verification services to the U.S. Social Security Administration and works with the federal Centers for Medicare and Medicaid Services to verify eligibility for health-insurance subsidies. These services include helping consumers check their Social Security benefits and request replacement Social Security cards,

[10] AnnaMaria Androitis, Michael Rapoport, and Robert McMillan, *'We've Been Breached': Inside the Equifax Hack*, THE WALL STREET JOURNAL (Sept. 18, 2017), https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318 (last accessed May 11, 2018).

as well as to verify eligibility for subsidies to buy health insurance under the Affordable Care Act.

45. Equifax recognizes that the value of its company is inextricably tied to its massive trove of consumer data. For that reason, Equifax has aggressively acquired companies with the goal of expanding into new markets and acquiring proprietary data sources.[11]

46. For example, in 2002 Equifax acquired Naviant Inc. for $135 million and gained access to Naviant's database of more than 100 million permission-based e-mail addresses.

47. In 2007, Equifax expanded its database of payroll information by acquiring TALX Corporation for $1.4 billion, which at the time held employment records on 142 million individuals. Following this acquisition, Equifax began offering a service called "The Work Number" that was designed to provide automated employment and income verification for prospective employers and allow anyone whose employer uses the service to provide proof of their income when purchasing a home or applying for a loan.[12] Equifax ultimately persuaded more than

[11] *Id*.

[12] Brian Krebs, *Equifax Breach Fallout: Your Salary History*, KREBS ON SECURITY (Oct. 17, 2017), https://krebsonsecurity.com/2017/10/equifax-breach-fallout-your-

7,000 employers to hand over salary details for this income verification system that encompasses nearly half of American workers.[13]

48. In 2009, Equifax paid $124 million in cash for IXI Corporation, a company specializing in collecting, analyzing and delivering consumer wealth and asset data. In its 2009 Annual Report, Equifax stated that, "The data and intelligence we derive from our broad base of assets—200+ million U.S. credit files; 200+ million records at The Work Number; $10 trillion in consumer wealth data from IXI; the National Consumer Telecom & Utilities Exchange; and the 26 million files of small business information—are unique and not replicable."

49. In 2010, Equifax acquired Anakam, Inc., an authentication management vendor that offered products addressing online identify verification, credentialing, and two-factor authentication. This acquisition permitted Equifax to sell to businesses identity and authentication systems that utilized consumers' credit information in order to verify the consumer's identity.

---

salary-history/ (last accessed May 11, 2018) ("Krebs, *Equifax Breach Fallout: Your Salary History*").

[13] Stacy Cowley and Tara Siegel Bernard, *As Equifax Amassed Ever More Data, Safety Was a Sales Pitch*, THE NEW YORK TIMES (Sept. 23, 2017), https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html?smprod=nytcore-ipad&smid=nytcore-ipad-share#story-continues-2 (last accessed May 11, 2018).

50. In 2012, Equifax paid $1 billion to absorb the largest independent CRA in the U.S., Computer Science Corp., which held credit files in 15 U.S. states covering 20 percent of the country's population.

51. In 2014, Equifax acquired TDX Group, a UK-based debt-management firm, for $327 million in order to expand its debt-collection capabilities. In 2016, Equifax acquired Veda Group Limited, the leading provider of credit information and analysis in Australia and New Zealand, for $1.7 billion.

52. Equifax now maintains information on over 820 million individuals and 91 million businesses worldwide. It is publicly traded on the New York Stock Exchange (ticker symbol EFX), and generated revenues of $3.362 billion in 2017.

53. Equifax also sells information directly to small businesses, including business credit reports marketed as allowing businesses to track their credit activity and financial health. As of May 2018, Equifax was charging $99.95 for business credit reports.

54. Equifax's strategy of rapid expansion by adding new data sources and increasing profits came with one major caveat: Equifax was unwilling to make corresponding investments in data security to protect the highly-sensitive information it continued to accumulate. And this directive came straight from the top. As noted by *The New York Times* in a September 2017 article: "Equifax's chief

executive had a simple strategy when he joined more than a decade ago: Gather as much personal data as possible and find new ways to sell it."[14]

Equifax Recognized the Importance of Data Security

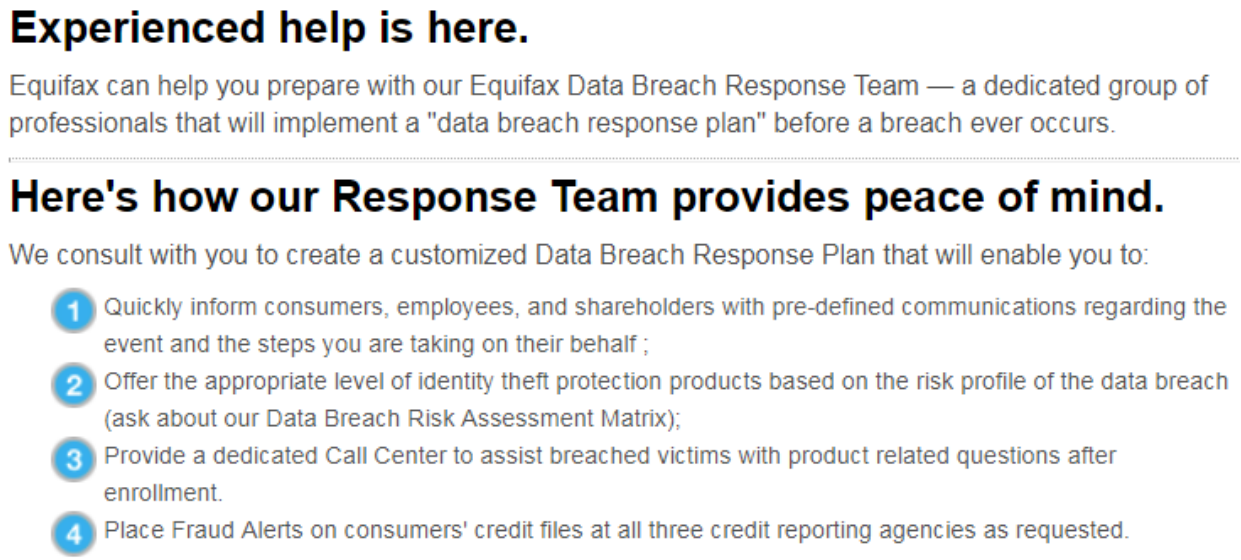
55. Equifax was well aware of the likelihood and repercussions of cybersecurity threats, including data breaches, having observed numerous other well-publicized data breaches involving major corporations over the last decade plus. In fact, Equifax sought to capitalize on the increase in the number of breaches by spending nearly $100 million since 2013 to acquire two identity theft protection and resolution companies—Trusted ID and ID Watchdog—to bolster its data breach response and product offerings.

56. As evidenced by its own product offerings, Equifax held itself out as a leader and expert in anticipating and combatting such threats and developed and sold "data breach solutions" to consumers and businesses to combat the "great risk of identity theft and fraud." Equifax even maintained a dedicated landing page to sell products and services specifically tailored to a data breach: www.equifax.com/help/data-breach-solutions.

[14] *Id.*

57. In its marketing materials, copied below, Equifax states: "You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events every day. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market."

58. Equifax has also touted its "Data Breach Response Team" which includes a "dedicated group of professionals that will implement a 'data breach response plan' before a breach ever occurs" including informing "consumers, employees, and shareholders with pre-defined communications" regarding the breach, offering identity theft protection products, providing a dedicated call center to assist breach victims, and placing fraud alerts on consumers' credit files.



Experienced help is here.

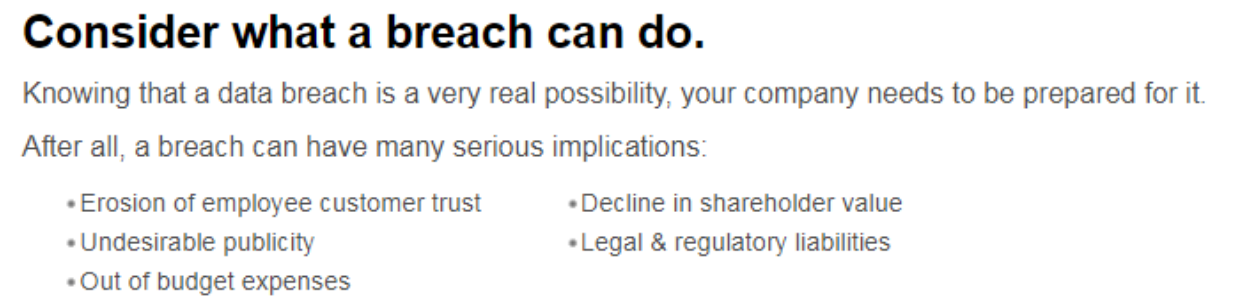
Equifax can help you prepare with our Equifax Data Breach Response Team — a dedicated group of professionals that will implement a "data breach response plan" before a breach ever occurs.

Here's how our Response Team provides peace of mind.

We consult with you to create a customized Data Breach Response Plan that will enable you to:

1. Quickly inform consumers, employees, and shareholders with pre-defined communications regarding the event and the steps you are taking on their behalf ;
2. Offer the appropriate level of identity theft protection products based on the risk profile of the data breach (ask about our Data Breach Risk Assessment Matrix);
3. Provide a dedicated Call Center to assist breached victims with product related questions after enrollment.
4. Place Fraud Alerts on consumers' credit files at all three credit reporting agencies as requested.

59. Equifax even summarized some of the repercussions of a data breach, including the erosion of employee and customer trust, decline in shareholder value, undesirable publicity, legal and regulatory liabilities, and out of budget expenses.



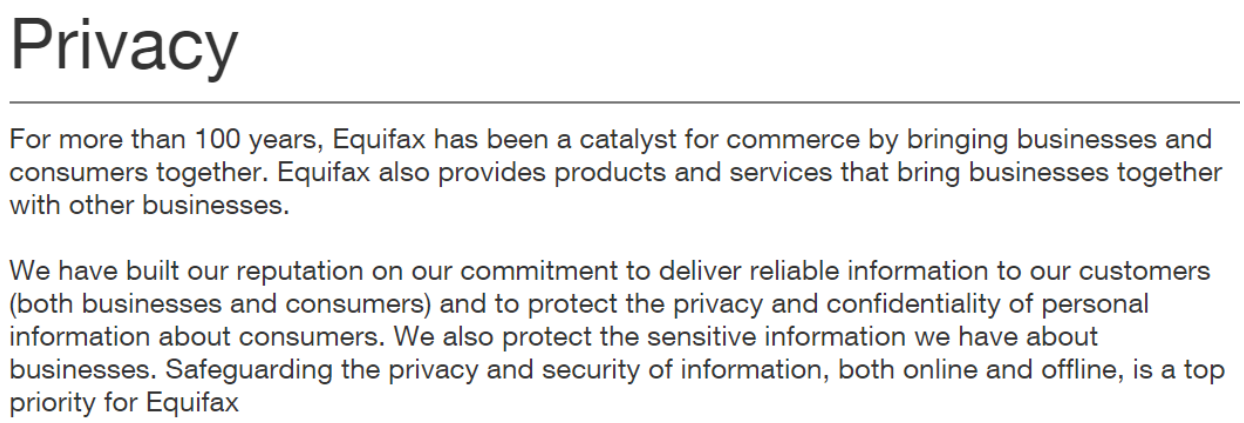
Consider what a breach can do.

Knowing that a data breach is a very real possibility, your company needs to be prepared for it. After all, a breach can have many serious implications:

- Erosion of employee customer trust
- Undesirable publicity
- Out of budget expenses
- Decline in shareholder value
- Legal & regulatory liabilities

60. Equifax also made representations to consumers regarding its data privacy practices. On its website, Equifax's summary statement of its Privacy Policy states: "For more than 100 years, Equifax has been a catalyst for commerce by bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses. We have built our

reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."[15]



Privacy

For more than 100 years, Equifax has been a catalyst for commerce by bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses.

We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax

61. The full text of Equifax's Privacy Policy states, among other things, that Equifax "restrict[s] access to personally identifiable information . . . that is collected about you to only those who have a need to know that information in connection with the purpose for which it is collected and used."

62. Equifax agreed it would "take reasonable steps to . . . [u]se safe and secure systems, including physical, administrative, and technical security procedures to safeguard the information about you." It agreed that "we have security protocols

[15] http://www.equifax.com/privacy/ (last accessed May 11, 2018).

and measures in place to protect the personally identifiable information . . . and other information we maintain about you from unauthorized access or alteration. These measures include internal and external firewalls, physical security and technological security measures, and encryption of certain data. When personally identifiable information is disposed of, it is disposed of in a secure manner."

63. Equifax's Privacy Policy further states: "We will not disclose your personal information to third parties except to provide you with the disclosure or service you request, or under certain circumstances as described in this policy."

64. In its Form 10-K from 2016, Equifax claimed that it was a "trusted steward and advocate for our customers and consumers" and stated that it was "continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives, while simultaneously delivering security for our services." The following year, Equifax included: "Data is at the core of our value proposition and the protection and safeguarding of that information is paramount."

65. Equifax also imposed stringent requirements on the businesses that purchase consumer information from Equifax, explicitly recognizing the parties' collective duty to protect consumer information. For example, in its form Broker Subscription Agreement, Equifax requires that:

a. "only Authorized Users can order or have access to" protected information;

b. credit reports are not provided "to any third party except as permitted";

c. protected information "must be encrypted when not in use and all printed [protected information] must be stored in a secure, locked container when not in use, and must be completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose";

d. protected information must be encrypted with: "Advanced Encryption Standard (AES), minimum 128-bit key or Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms";

e. Equifax's business partner must "monitor compliance" with these obligations "and immediately notify EQUIFAX if [the business partner] suspects or knows of any unauthorized access or attempt to access the" protected information;

f. Equifax's business partner must "not ship hardware or software . . . to third parties without deleting . . . any consumer information";

g. Equifax's business partner must "use commercially reasonable efforts to assure data security when disposing of any consumer report information";

h. "Such efforts must include the use of those procedures issued by [applicable agencies], "e.g. the Federal Trade Commission . . ."

66. With regard to network security, Equifax acknowledges and requires that its business partners must "use commercially reasonable efforts to protect EQUIFAX Information when stored on servers", subject to the following requirements:

- "EQUIFAX Information must be protected by multiple layers of network security, including but not limited to, firewalls, routers, intrusion detection device";
- "secure access (both physical and network) to systems storing EQUIFAX Information must include authentication and passwords that are changed at least every 90 days";
- "all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available."

67. In 2017, Equifax's Chief Information Security Officer ("CISO"), Susan Mauldin, gave an interview about "how the role of a Chief Information Security Officer has evolved in response to growing cybersecurity threats."[16] In the interview, Ms. Mauldin discussed at length her methods for addressing expected cybersecurity threats, stating that "[w]e spend our time looking for threats against a company. We look for things that might be active inside the company that would cause us concern, and then of course we look to respond—detecting, containing and deflecting those threats."[17] She went on to outline some of her "best practices" for combatting cybersecurity threats. It was later revealed that Ms. Mauldin had no formal training in information systems or cybersecurity; rather, her training was in music composition.

[16] http://archive.is/6M8mg (last accessed May 11, 2018). Shortly after the breach, the active article was removed from the internet, and only an archive of the file remains.

[17] *Id*.

68. Equifax's awareness of the importance of data security was bolstered in part by its observation of numerous other well-publicized data breaches involving major corporations being targeted for consumer information in the years preceding the Equifax breach.

69. Through a series of data breaches extending back to 2013, more than three billion Yahoo user accounts were compromised when the real names, addresses, and dates of birth were stolen. The hackers also stole passwords, both encrypted and unencrypted, and security questions and answers.

70. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target Stores and The Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.

71. In summer 2014, a data breach of JP Morgan Chase compromised the data of 76 million American households and 7 million small businesses. Breached data included contact information (names, addresses, phone numbers, and email addresses) as well as "internal information about the users."

72. In early 2015, Anthem, the second-largest health insurer in the United States, suffered a data breach that exposed the names, addresses, Social Security

numbers, dates of birth and employment histories of nearly 80 million current and former plan members.

73. In September 2015, credit reporting agency Experian, Equifax's largest competitor, acknowledged that an unauthorized party accessed one of its servers containing the names, addresses, Social Security numbers, dates of birth, driver's license, military ID, and/or passport numbers, and additional information of more than 15 million consumers over a period of two years.

74. Dozens of other data breaches over the past few years were well known to information technology ("IT") and security professionals across the country, and particularly Equifax. Unfortunately, Equifax did not view these breaches as cautionary tales, but rather as another avenue to profit from businesses and consumers concerned with fraud. Equifax's CEO Richard Smith admitted as much in an August 2017 speech where he referred to consumer fraud as a "huge opportunity" and "massive, growing business" for Equifax.[18]

[18] Jim Puzzanghera, *Senators Slam Equifax for making money off massive data breach and no-bid IRS contract*, LOS ANGELES TIMES (Oct. 4, 2017), http://www.latimes.com/business/la-fi-equifax-senate-20171004-story.html (last accessed May 11, 2018) ("Puzzanghera, *Senators Slam Equifax*"); Megan Leonhardt, *Equifax Is Going to Make Millions Off Its Own Data Breach*, TIME (Oct. 4, 2017), http://time.com/money/4969163/equifax-hearing-elizabeth-warren-richard-smith/ (last accessed May 11, 2018).

Equifax Has a History of Inadequate Data Security Practices

75. Given the amount of sensitive data it compiles and stores, Equifax was well aware it was a target, but nonetheless refused to implement best practices relating to data security—as demonstrated by the numerous data security lapses Equifax has experienced over the last 10 years.

76. In 2010, tax forms mailed by Equifax's payroll vendor had Equifax employees' SSNs partially or fully viewable through the envelope's return address window. One affected Equifax employee stated "If they can't do this internally how are they going to be able to go to American Express and other companies and say we can mitigate your liability? They are first-hand delivering information for the fraudsters out there. It's so terribly sad. It's just unacceptable, especially from a credit bureau."[19]

77. In March of 2013, all three major credit reporting agencies acknowledged intrusions into their systems after information pertaining to celebrities and high-profile figures ended up on the *Exposed* website.[20] Attackers

[19] Elinor Mills, *Equifax tax forms expose worker Social Security numbers*, CNET (Feb. 11, 2010), http://www.cnet.com/news/equifax-tax-forms-expose-worker-social-security-numbers/ (last accessed May 11, 2018).

[20] David Bisson, *4 Credit Bureau Breaches that Predate the 2017 Equifax Hack*, TRIPWIRE (Sept. 14, 2017), https://www.tripwire.com/state-of-security/security-data-protection/4-credit-bureau-data-breaches-predate-2017-equifax-hack/ (last accessed May 11, 2018).

gained fraudulent and unauthorized access to credit reports and other personal sensitive information for former First Lady Michelle Obama, Paris Hilton, former Secretary of State Hillary Clinton, and former FBI Director Robert Mueller.[21] In addition, hackers gained access to publicly available information on individuals to answer security questions, which enabled them to bypass the credit bureaus' authentication measures.[22] This breach was called a "juvenile hack" but proved that the credit reporting agencies struggled to "properly authenticat[e] users attempting to view their credit report."[23] Despite this incident, Equifax stated in its February 28, 2014 Annual Report that it "ha[d] not experienced any material breach of cybersecurity."

78. Starting in April 2013, an IP address operator was able to obtain credit reports using sufficient personal information to meet Equifax's identity verification process. On January 31, 2014, Equifax's security team discovered a suspicious pattern of inquiries and blocked the IP address from further access. Equifax acknowledged that from April 2013 to January 31, 2014, the IP address operator

[21] Robert Westervelt, *Equifax, Other Credit Bureaus Acknowledge Data Breach*, CRN (Mar. 13, 2013), https://www.crn.com/news/security/240150683/equifax-other-credit-bureaus-acknowledge-data-breach.htm (last accessed May 11, 2018).
[22] *Id*.
[23] *Id*.

may have made unauthorized and fraudulent requests for Equifax credit reports. Equifax reported the suspicious activity to the FBI and offered affected individuals a one-year subscription to its credit monitoring service.[24]

79. In 2014, Equifax left private encryption keys on its server, allowing anyone who accessed the server to obtain the keys and decrypt encrypted data into its original form.[25]

80. In 2015, Equifax exposed consumer data as a result of another "technical error," this time one that "occurred during a software change."[26] Also in March 2015, Equifax sent a Maine woman the full credit reports of more than 300 other individuals, which exposed their social security numbers, dates of birth, current and previous addresses, creditor information, and bank and loan account numbers, among other sensitive information. The woman told reporters "I'm not supposed to

[24] Letter from Equifax Legal Department to Attorney General Joseph Foster Regarding Security Breach Notification (Mar. 5, 2014) at 1, https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf (last accessed May 11, 2018) .

[25] Brian Krebs (@briankrebs), TWITTER (Sept. 15, 2017 8:59 AM), https://twitter.com/briankrebs/status/908722014449520642 (last accessed May 11, 2018).

[26] Letter from King & Spalding LLP to Attorney General Joseph Foster Regarding Data Incident Notification (Apr. 2, 2015) at 1, https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20150402.pdf (last accessed May 11, 2018).

have this information, this is unbelievable, someone has messed up."[27] In response, Equifax's Vice President of Corporate Communications, Tim Klein, said, "This is a high priority. Obviously, this is a serious situation. I'm going to get our security and forensics teams involved."

81. In 2016, a security researcher found a common vulnerability known as cross-site scripting (XSS) on the main Equifax website. XSS bugs allow attackers to send specially-crafted links to Equifax customers and, if the target clicks through and is logged into the site, their username and password can be revealed to the hacker. The researcher reported that the bug had not been fixed even months after it was initially made known to Equifax.[28]

82. In May 2016, it was discovered that a product offered by Equifax's subsidiary company Equifax Workforce Solutions, Inc. (d/b/a TALX), a purveyor of electronic W-2 forms accessible for download for many companies, contained a major security vulnerability that allowed data thieves "to access W-2 data merely by

---

[27] Jon Chrisos, *Credit agency mistakenly sends 300 confidential reports to Maine woman*, BANGOR DAILY NEWS (March 19, 2015), http://bangordailynews.com/2015/03/19/news/state/credit-agency-mistakenly-sends-300-confidential-reports-to-maine-woman/ (last accessed May 11, 2018).

[28] Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES (Sept. 8, 2017) https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#671ed1c677c0 (last accessed May 11, 2018).

entering at Equifax's portal the employee's default PIN code, which was nothing more than the last four digits of the employee's Social Security number and their four-digit birth year" including employees of grocery chain Kroger.[29] That same month, Stanford University identified approximately 600 employees whose W-2 data was hacked through Equifax's W-2 Express portal.[30] Again in April of 2016, Northwestern University notified approximately 150 employees whose salary and tax data was breached through Equifax.[31]

83. In August of 2016, in light of all of these previous breaches, institutional investor advisor MSCI, Inc. cautioned that Equifax was ill-prepared to face the "increasing frequency and sophistication of data breaches."[32] As a result,

---

[29] Brian Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY (May 16, 2016), https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/ (last accessed May 11, 2018) ("Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*").

[30] Hannah Knowles, *University employees vulnerable after tax data breach*, THE STANFORD DAILY (Apr. 12, 2016), https://www.stanforddaily.com/2016/04/12/university-employees-vulnerable-after-tax-data-breach/(last accessed May 11, 2018); *see also* Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*.

[31] See Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*.

[32] Asjylyn Loder, *A Warning Shot on Equifax: Index Provider Flagged Security Issues Last Year*, THE WALL STREET JOURNAL (Oct. 6, 2017), https://www.wsj.com/articles/a-warning-shot-on-equifax-index-provider-flagged-security-issues-last-year-1507292590 (last accessed May 11, 2018).

MSCI downgraded Equifax to a "CCC" grade for its environmental, social and governance risks—the lowest rating used by the company.

84. Several months later, in December of 2016, just a few months before the breach at issue in this case, a security researcher warned Equifax that one of its public-facing websites "displayed several search fields, and anyone—with no authentication whatsoever—could force the site to display the personal data of Equifax's customers."[33] The researcher was able to access full names, Social Security numbers, birth dates, and city and state of residence information for affected consumers. The flaw was discovered on a webpage that appeared to be a portal for employees. The webpage contained multiple search boxes and allowed anyone to force the site to display the personal information of Equifax customers and credentials that were needed to access the search page. The researcher was also able to take control of several Equifax servers and found that the servers were running outdated software that was vulnerable to breach. It took the company six months to patch that vulnerability.[34]

---

[33] Lorenzo Franceschi-Bicchierai, *Equifax Was Warned*, VICE (Oct. 26, 2017), https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning (last accessed May 11, 2018) ("Franceschi-Bicchierai, *Equifax Was Warned*").

[34] George Cox, *Equifax suffers another security breach*, THE SPECTRUM (Nov. 8, 2017),

85. The next month, in January of 2017, Equifax received a report that a member of credit monitoring service LifeLock was able to view another person's credit report. Equifax researched the issue and acknowledged that credit information of a small number of LifeLock members was inadvertently sent to another member's online portal "as the result of a technical issue."[35]

86. Given the condition of Equifax's security and software management, multiple third parties concluded that, given the condition of its security and software management, Equifax was highly susceptible to a breach in 2017.

87. For example, four independent analyses of Equifax cybersecurity, conducted either before or immediately after the breach, identified important weaknesses including that Equifax "was behind on basic maintenance of websites that could have been involved in transmitting sensitive consumer information and scored poorly in areas" highly relevant to potential breaches.[36]

---

https://www.thespectrum.com/story/life/features/mesquite/2017/11/08/equifax-suffers-another-security-breach/842717001/ (last accessed May 11, 2018).

[35] Letter from King & Spalding LLP to Attorney General Joseph Foster Regarding Data Incident Notification (Feb. 8, 2017), https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20170208.pdf (last accessed May 11, 2018).

[36] AnnaMaria Androitis and Robert McMillan, *Equifax Security Showed Signs of Trouble Months Before Hack*, THE WALL STREET JOURNAL (Sept. 26, 2017), https://www.wsj.com/article_email/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947-1MyQjAxMTA3OTIyNjUyMzY5Wj/ (last

88. In April 2017—the month before the breach—Cyence, a cyber-risk analysis firm, "rated the danger of a data breach at Equifax during the next 12 months at 50%. It also found the company performed poorly when compared with other financial-services companies."[37]

89. SecurityScorecard, another security monitoring firm, identified the precise weakness that was used by the hackers to breach the Equifax system, reporting that "Equifax used older software—such as the Apache Struts tool kit . . . and often seemed slow to install patches."[38]

90. An outside review by FICO rated Equifax's "enterprise security score" based on three elements: hardware, network security, and web services. The score declined from 550 out of 800 at the beginning of 2017 to 475 in mid-July 2017 when the breach had already occurred. The FICO analysis found that public-facing websites run by Equifax had expired certificates, and there were errors in the chain of certificates and other web-security issues. Certificates are used to validate the

---

accessed May 11, 2018). *See also Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information* (Feb. 7, 2018), https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf (last accessed May 11, 2018) ("Warren Report").

[37] *Id.*

[38] *Id.*

connection between a user's web browser and an HTTPS web server, allowing users to know that their connection to a website is legitimate and secure.

91. A fourth independent review released just after the breach was revealed identified significant problems with Equifax cybersecurity. This report by BitSight Technologies gave the company an "'F" in application security and a "D" for software patching.[39]

The Equifax Data Breach

92. Equifax maintains a consumer dispute website where consumers can go online to dispute inaccurate information contained on their credit reports. This website runs on Apache Struts software, which is a popular programming framework for building web applications in Java.

93. Apache Struts makes it "easier for developers to build top-to-bottom custom websites" and it "can handle everything from interactive screens and logins, to web apps and database management."[40]Apache Struts is "open source" meaning that the source code is made freely available and may be redistributed and modified by anyone who wants to use it.

---

[39] See Warren Report at 5.

[40] Ben Popken, *Equifax Hackers Exploited Months-Old Flaw*, NBC NEWS (Sept. 14, 2017), https://www.nbcnews.com/business/consumer/how-did-equifax-hack-even-happen-n801331 (last accessed May 11, 2018) ("Popken, *Equifax Hackers Exploited Months-Old Flaw*").

94. While Apache Struts has been widely used by companies and government agencies for years, and is currently in use by at least 65% of Fortune 100 companies,[41] its popularity and expansive capabilities leaves it vulnerable to cyberattacks. Indeed, because the software "touches all aspects of a company's website," once hackers locate a vulnerability, they gain "unfettered access" to the underlying system and can "execute commands just like they were the administrators." In other words, "they basically control the system."[42]

95. On March 6, 2017, a serious vulnerability in the Apache software was discovered and reported. The discovery of this vulnerability was described as a "hair on fire moment" in the IT world that caused all affected IT professionals to scramble for a fix.[43]

96. On March 7, 2017, one day after the vulnerability in the Apache software was discovered, the Apache Software Foundation issued a "patch" to

[41] Keith Collins, *The hackers who broke into Equifax exploited a flaw in open-source server software*, QUARTZ (Sept. 8, 2017), https://qz.com/1073221/the-hackers-who-broke-into-equifax-exploited-a-nine-year-old-security-flaw/ (last revised Sept. 14, 2017) (last accessed May 11, 2018).

[42] See Popken, *Equifax Hackers Exploited Months-Old Flaw*.

[43] *Id*.

address the flaw, and warned its customers of the risk and the need to implement the patch.[44]

97. On March 8, 2017, Equifax received a specific and detailed warning from the Department of Homeland Security's U.S. Computer Emergency Readiness Team ("CERT") regarding the Apache Struts vulnerability and available patch.[45]

98. On March 9, 2017, Equifax disseminated the U.S. CERT notification internally by email, requesting that applicable personnel responsible for an Apache Struts installation upgrade their software. The Equifax security department required that patching occur within a 48-hour time period. However, Equifax's IT personnel did not properly utilize this patch, update its software, or otherwise address the vulnerability at that time.[46]

---

[44] Russell Grantham, *Equifax, software maker blame each other for opening door to hacks*, THE ATLANTA JOURNAL-CONSTITUTION (updated Sept. 29, 2017), http://www.ajc.com/business/equifax-software-maker-blame-each-other-for-opening-door-hackers/p5wJS5CgTLrmKUL59CTAjM/ (last accessed May 11, 2018).

[45] *Prepared Testimony of Richard F. Smith before the United States House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection* (October 3, 2017), https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf . ("Prepared Testimony of Richard F. Smith, (Oct. 3, 2017)").

[46] *Id.*

99. Ordinarily, applying a patch that is accompanied by "clear and simple" instructions is a straightforward proposition that provides an easy fix to prevent a serious problem.[47] Had Equifax properly applied the patch like thousands of other affected companies, the vulnerability exploited to perform the breach would have been fixed.[48]

100. The vulnerability and the fact that attackers sought to exploit it was widely-publicized. For example, tech blogs reported "a string of attacks that have escalated over the past 48 hours [where] hackers are actively exploiting a critical vulnerability that allows them to take almost complete control of Web servers used by banks, government agencies, and large Internet companies."[49] And many sources reported about the uptick in attacks against companies that had not yet installed the patch. Open source security company WhiteSource reported that "[t]he vulnerability was scored as critical (CVSS 10) [the highest grade], mainly due to how easy it is to

---

[47] Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017) https://www.wired.com/story/equifax-breach-no-excuse/ (last accessed May 11, 2018).

[48] *Id.*

[49] Dan Goodin, *Critical vulnerability under "massive" attack imperils high-impact sites*, ARS TECHNICA (Mar. 9, 2017), https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/ (last accessed May 11, 2018).

hack. And indeed reports from days after the Apache Struts March vulnerability was released showed hackers were exploiting it en masse."[50]

101. On March 15, 2017, Equifax ran scans that should have verified that the Apache Struts patch was properly installed. But Equifax failed to scan all of its systems and failed to discover the vulnerability that still lay at the heart of its systems. This failure to thoroughly scan its systems left Equifax open to the massive breach that would unfold over the next several months.

102. By the admission of Equifax's CEO Richard Smith at the time of the breach, Equifax's systems were infiltrated for the first time on May 13, 2017, well over two months after the Apache Struts patch was first made available.

103. In addition to lacking the necessary safeguards to secure its most valuable "core" data, such as records containing consumer identities and Social Security numbers, Equifax did not have adequate monitoring systems and controls in place to detect the unauthorized infiltration after it occurred. Indeed, Equifax, like any company its size storing valuable data, should have had robust protections in

[50] Ayala Goldstein, *The Equifax Breach: Who's to Blame?*, WHITESOURCE (Sept. 10, 2017), https://www.whitesourcesoftware.com/whitesource-blog/equifax-data-breach/ (last accessed May 11, 2018).

place to detect and terminate a successful intrusion long before access and exfiltration can expand to hundreds of millions of consumer files.

104. Unfortunately, Equifax did not have these necessary controls in place, and between May 13 and July 30, 2017, hackers were able to utilize simple commands to determine the credentials of network accounts at Equifax to access and infiltrate the sensitive personal information of approximately 147.9 million American consumers.[51]

Equifax Discovers the Data Breach

105. On July 29, 2017, over four and a half months after the CERT notification about the Apache Struts vulnerability was issued, Equifax's security team noticed "suspicious network traffic" connected to its consumer dispute website.[52]

106. The security department continued investigating the abnormal activity through July 30, 2017. In response, the Equifax security team deactivated the consumer dispute website and took it entirely offline.

---

[51] AnnaMaria Androitis and Robert McMillan, *Hackers Entered Equifax Systems in March*, THE WALL STREET JOURNAL (updated Sept. 20, 2017), https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617 (last accessed May 11, 2018).

[52] See Prepared Testimony of Richard F. Smith (Oct. 3, 2017).

107. Equifax's CEO Richard Smith was informed of the breach the following day on July 31, 2017. Equifax did not notify the chairman of its board of directors until August 22, 2017, and waited two more days to inform the full board.

108. On August 1, 2017, three days after Equifax first noticed the breach, three high-level Equifax executives sold millions of dollars' worth of Equifax stock. Equifax's Chief Financial Officer John Gamble sold $946,374 of stock. Equifax's president of U.S. Information Relations, Joseph Loughran, sold $584,099 of stock. Equifax's President of Workforce Solutions, Rodolfo Ploder, sold $250,458 of stock. And on August 25, 2017, two weeks before Equifax publicly announced the breach, Chief Information Officer Jun Ying sold $950,000 of stock.

109. None of those transactions were part of previously scheduled 10b5-1 trading plans. Equifax claims that these executives did not know of the breach at the time they sold their stock.

110. On August 2, 2017, Equifax informed the Federal Bureau of Investigation about the breach and retained the law firm King & Spalding LLP to guide its investigation of the breach. Equifax also hired the cybersecurity forensic firm Mandiant to analyze and investigate the suspicious activity on its network.

111. Over the next several weeks, Mandiant and Equifax's internal security department analyzed forensic data to determine the nature and scope of the

suspicious activity. It was determined that Equifax had been subject to cyber-intrusions that resulted in a breach of Equifax's IT systems.

112. In accordance with Equifax's internal policies, the company classified the breach as a "critical incident" and formed a crisis action team, comprised of security, legal, and IT personnel.

113. Equifax designated the response to the breach as "Project Sierra," and instructed those working on Project Sierra that information related to the project was confidential and should not be shared with anyone outside of Equifax's crisis action team.

114. On August 10, 2017, approximately two weeks after discovering the breach, Equifax purchased identity theft security service ID Watchdog for $62 million. ID Watchdog offers services that monitor consumers' credit and warn of potential identity theft for $15 to $25 per month. That same month, well after he was aware of both the Equifax breach and the ID Watchdog acquisition, Equifax CEO Richard Smith reaffirmed in a speech, "Fraud is a huge opportunity for us—it's a massive, growing business for us."[53]

[53] See Puzzanghera, *Senators Slam Equifax*.

115. On August 11, 2017, the forensic investigation revealed that certain "dispute documents" submitted by customers to dispute information in their consumer file were accessed, as well as "a large amount" of consumers' personal identifying information and "potentially other data tables."

116. Several days later, Equifax learned through Mandiant that the extensive personal identifying information had not only been accessed but also stolen (*i.e.*, exfiltrated from its systems), and that "large volumes" of consumer data had been compromised.

117. Between August 12 and 15, 2017, Project Sierra team members changed administrative credentials for hundreds of internal databases. The so-called "password reset" required the assistance of a broader group of Equifax IT employees who were not informed of the breach.

118. Equifax also established a notification and remediation plan for the millions of consumers affected by the breach. This effort, which the company designated "Project Sparta," involved setting up a website for consumers to determine whether they were affected by the breach, developing a suite of protective tools for consumers, and staffing call centers.

119. Project Sparta was kept separate from Project Sierra to limit the number of people who knew that Equifax itself had been breached. Those Equifax employees

who were only part of Project Sparta were not told that Equifax had been breached, but were instead told that they were assisting with a "business opportunity" whereby Equifax was working for an unnamed client that had experienced a large data breach.

120. Equifax decided to handle much of the work for Project Sparta through its own Global Consumer Solutions business unit, which developed and sold various personal security and identity theft defense products and services to clients.

121. By September 4, 2017, Equifax had compiled a list of the roughly 143 million consumers whose personal information had been stolen. Since that time, Equifax has identified additional consumer victims. On May 7, 2018, Equifax submitted a "statement for the record" to the Securities and Exchange Commission more fully detailing the breakdown of stolen Personal Information.

Information Stolen	**Approximate Number of Impacted U.S. Customers**
Name	146.6 million
Date of Birth	146.6 million
Social Security Number	145.5 million
Address Information	99 million
Gender	27.3 million
Phone Number	20.3 million
Driver's License Number	17.6 million
Email Address	1.8 million

Payment Card Number and Expiration Date	209,000
Tax ID	97,500
Driver's License State	27,000

122. As alleged further below, the highly sensitive nature of the Personal Information stolen and unprecedented scale of the breach is likely to affect a significant portion of the U.S. population for years to come.

Equifax's Inadequate Data Security Practices

123. The Equifax breach was the inevitable result of a top-down policy to prioritize growth and profits over data security. The technical deficiencies and weaknesses that permitted unfettered access to Equifax's systems demonstrate how little priority was given to even rudimentary data security protocols, despite Equifax's role as one of the largest custodians of consumer data in the world.

124. In February 2018, Senator Elizabeth Warren's office released the results of a 5-month investigative report setting forth a number of findings regarding the breach, including Equifax's inadequate data security practices that contributed to the breach (the "Warren Report").

125. The investigation found that "the breach was made possible because Equifax adopted weak cybersecurity measures that failed to protect consumer data—a symptom of what appeared to be the low priority afforded cybersecurity by

company leaders. The CEO at the time of the breach, Richard Smith, testified that despite record profits in recent years, Equifax spent only a fraction of its budget on cybersecurity—approximately 3 percent of its operating revenue over the last three years."[54]

126. After consultation with experts, the Warren Report concluded that companies such as Equifax that hold large amounts of sensitive data should have multiple layers of cybersecurity, including (1) frequently updated tools to prevent hackers from breaching their systems; (2) controls that limit hackers' ability to move throughout their systems in the event of an initial breach; (3) restrictions on hackers' ability to access sensitive data in the event of an initial breach; and (4) procedures to monitor and log all unauthorized access in order to stop the intrusion as quickly as possible.[55] The report stated that, "Despite collecting data on hundreds of millions of Americans without their permission, Equifax failed to fully and effectively adopt any of these four security measures."[56]

127. The Warren Report identified six areas where Equifax's cybersecurity measures were particularly deficient:

---

[54] See Warren Report at 3.

[55] *Id.*

[56] *Id.*

a. ***Faulty Patch Management Procedures***—"For many vulnerabilities that arise in its software and applications, Equifax only has to deploy a software 'patch' that will fix the vulnerability and restrict access to the susceptible system. . . . Yet Equifax let numerous software vulnerabilities sit un-patched for months at a time, leaving weaknesses through which hackers could gain access."[57]

b. ***Feeble Monitoring of Endpoint and Email Security***—Endpoint security refers to protecting a corporate network when it is accessed via remote devices like laptops and mobile devices, as such devices can create a potential entry point for security threats. "Equifax failed to adopt strict endpoint and email security measures" to secure each endpoint on the network created by these devices.[58]

c. ***Exposure of Sensitive Information***—Equifax stored and "retained sensitive consumer information on easily accessible systems" rather than segregating the most sensitive information into locations designed to limit access and maximize security.[59]

d. ***Weak Network Segmentation***—Equifax "failed to put security measures in place that would prevent hackers from jumping from insecure, internet-facing systems to backend databases that contain more valuable data. . . . Equifax's network segmentation measures failed to keep hackers from accessing consumer information because the company did not adopt adequately strict measures to protect valuable data."[60]

e. ***Inadequate Credentialing***—"Equifax's cybersecurity failures extended to their internal security. Each user on Equifax's system receives a set of privileges. Under a strict security standard, Equifax would limit access to the most critical databases to just a handful of necessary users. This would protect the company from internal attacks and further bolster the company's overall data security regime. After

[57] *Id*.

[58] *Id*.

[59] *Id*.

[60] *Id*.

gaining access to Equifax's system, hackers then acquired user credentials—a username and password—and accessed a huge quantity of sensitive information using just those credentials. The company did not adopt adequately strict security measures to properly restrict user access to sensitive data."[61]

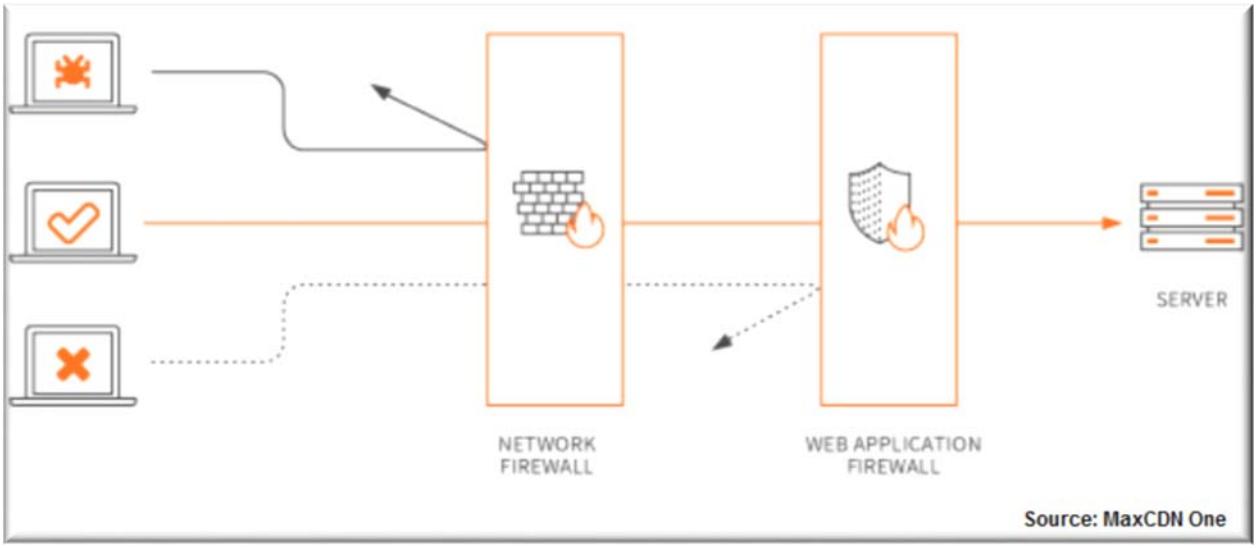
f. ***Inadequate Logging***—"Equifax neglected the use of robust logging techniques that could have allowed the company to expel the hackers from their systems and limited the size and scope of the data breach. Logging is a simple but crucial cybersecurity technique in which companies monitor their systems, continuously logging network access in order to identify unauthorized users. . . . Equifax allowed hackers to continuously access sensitive data for over 75 days, in part because the company failed to adopt effective logging techniques and other security measures."[62]

128. Equifax's failures to adopt these industry-standard measures were more than mere mistakes, they were calculated decisions by Equifax executives to skirt data security in favor of paying out annual dividends. As noted in the Warren Report, "Equifax's goal, as stated by its CEO just weeks before he disclosed the breach, was to go from '$4 billion in revenue to $8 billion' in approximately 5 years. Equifax prioritized growth and profits—but did not appear to prioritize cybersecurity."[63]

129. Other cybersecurity analysists have pointed to additional failures by Equifax. For example, Equifax's consumer dispute website did not make use of a web application firewall ("WAF") that would have served as a second line of defense

[61] *Id*. at 4.
[62] *Id*.
[63] *Id*.

by intercepting and analyzing all HTTP requests before they reached the web server for processing.[64]



130. Because WAFs can detect and stop outside attacks resulting from vulnerabilities inherent in web applications, implementation of a WAF like would have prevented the breach from occurring.[65] Equifax's consumer dispute website, contrary to best practices, had no WAF in place at the time of breach.

131. Additionally, there is evidence that Equifax used outdated security certificates, which permitted the hackers to easily bypass Equifax's login protocols,

---

[64] Amos Ndegwa, *What is a Web Application Firewall?*, MAXCDN (May 31, 2016), https://www.maxcdn.com/one/visual-glossary/web-application-firewall/ (last accessed May 11, 2018); Tushar Richabadas, *"WAF Prevents Massive Data Breach at Equifax" . . . The headline that could have been, but wasn't . . ."*, BARRACUDA (Sept. 22, 2017)

[65] *Id.*

as well as an outdated operating system and infrastructure that was ill-equipped to protect against modern threats. And because Equifax did not have adequate network segmentation, hackers were able to move from the initial point of entry to other IT systems.

132. But even the existence of these major security deficiencies does not explain how hackers were able to move around Equifax's servers unnoticed for more than 75 days while exfiltrating tens of millions of consumer records. Indeed, any routine and competent monitoring of its consumer dispute portal would have revealed to Equifax that there was significant irregular activity taking place on its servers.

133. Equifax's deficiencies in cybersecurity were well known and widely lamented even within Equifax itself. As one former employee and cybersecurity engineer stated, "The degree of risk [Equifax] assumes is found, by most of the IT staff who worked elsewhere, to be preposterous."[66]

134. Another former Equifax employee involved in a cybersecurity audit of Equifax by Deloitte said, "Nobody took that security audit seriously. Every time

[66] *Id.*

there was a discussion about doing something, we had a tough time to get management to understand what we were even asking."[67]

135. The lack of basic safeguards on Equifax's systems and the company's failure to implement even minimal, industry-standard practices further highlights the glaring lack of care exercised by Equifax in protecting its massive trove of consumer data. Clearly cybersecurity was not a priority at Equifax—even after multiple breaches and warnings had put Equifax on notice that the data it was entrusted to safeguard was extremely vulnerable.

Equifax's Botched Public Disclosure and Response to the Breach

136. Equifax was first warned about the Apache Struts vulnerability on March 8, 2017, the breach occurred on May 13, 2017, and Equifax first observed suspicious network traffic on July 29, 2017. Yet Equifax waited until September 7, 2017, to publicly announce the breach in a nationwide press release. By waiting approximately 7 weeks after Equifax discovered the breach to notify consumers, Equifax deprived consumers of an opportunity to take immediate precautionary measures to protect themselves from identity theft and fraud.

137. Equifax's press release, which did not mention when the breach had occurred, conceded that for 143 million consumers, "[t]he information accessed

[67] *Id*.

primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers."

138. By using the term "accessed" instead of "stolen" or "exfiltrated", Equifax intentionally failed to convey the seriousness of the breach and that consumers' information was already in the possession of an unauthorized third party.

139. At the time of the announcement, then-CEO Richard Smith wrote that Equifax is "focused on consumer protection and [has] developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

140. Post-breach, Equifax's website contained a link where consumers could provide their last name and the last six digits of their Social Security number to see if their Personal Information was exposed in the breach. This link was circulated by countless online media companies, blogs, and social networks.

141. Contrary to the promises made by Equifax, the website did not indicate whether one's information had been potentially impacted—instead, it told most consumers that they "may" have been compromised.

142. The application then provided consumers with a date in the future when they could enroll in one year of "TrustedID Premier," an Equifax credit monitoring service. However, to sign up for the service, the consumer was required to sign an

agreement that included an arbitration clause and class action waiver, and also stated that Equifax could charge the consumer for the year of TrustedID Premier if they did not cancel the service within a year. After a public outcry, Equifax retreated and ultimately removed these requirements from its fine print.

143. Equifax's data breach response website was universally panned not only as unhelpful, but also as a "stalling tactic" and a "sham." According to Brian Krebs, a leading cybersecurity expert:

> As noted in yesterday's breaking story on this breach, the Web site that Equifax advertised as the place where concerned Americans could go to find out whether they were impacted by this breach — equifaxsecurity2017.com — is completely broken at best, and little more than a stalling tactic or sham at worst.
>
> In the early hours after the breach announcement, the site was being flagged by various browsers as a phishing threat. In some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones. Others (myself included) received not a yes or no answer to the question of whether we were impacted, but instead a message that credit monitoring service we were eligible for was not available and to check back later in the month. The site asked users to enter their last name and last six digits of their SSN, but at the prompting of a reader's comment I confirmed that just entering gibberish names and numbers produced the same result as the one I saw when I entered my real information: Come back on Sept. 13.[68]

[68] Brian Krebs, *Equifax Breach Response Turns Dumpster Fire*, KREBS ON SECURITY (Sept. 8, 2017), https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire (last accessed May 11, 2018).

144. In the wake of this problematic rollout, Equifax's website and phone lines crashed repeatedly. The website was overwhelmed, frequently generating system error messages.[69] Numerous consumers had "difficulty in reaching Equifax's call centers and in accessing their security freeze PIN, as well as lengthy hold times, dropped calls, and agents not calling back as promised."[70]

145. There were numerous reports that Equifax's call center representatives did not know how to answer basic questions regarding credit freezes and provided an alternate number to call that did not direct callers to a service that had the answers, but was actually a "triple-X hardcore service."[71]

146. Consumers received different answers as to whether they had been impacted depending on whether they had accessed the site through a computer or mobile device, and the website gave the same information to consumers about whether they had been affected even when they entered incorrect or false information.[72] As recently as April 2018, this Equifax website tool still did not

---

[69] *Id*.

[70] See Warren Report at 8 (citations and quotations omitted).

[71] Ron Lieber, *How to Protect Yourself After the Equifax Breach*, THE NEW YORK TIMES (updated Oct. 16, 2017), https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html (last accessed May 11, 2018) ("Lieber, *How to Protect Yourself After the Equifax Breach*").

[72] Letter from United States House Committee on Energy and Commerce to Richard F. Smith (September 12, 2017),

function properly to allow consumers to confirm whether they were victims of the data breach.

147. Richard Smith admitted that Equifax was "disappointed" with the rollout of its website and call centers, and that it "struggled with the initial effort" to assist consumers after the breach.[73]

148. To make matters even worse, the website Equifax set up to help consumers find out whether they were impacted by the breach was itself found to contain security flaws making it vulnerable to hackers. Equifax also directed consumers to a fake phishing site via its official Twitter feed, directing users to check if they had been breached at the website securityequifax2017.com, instead of equifaxsecurity2017.com.

149. The breach led to scammers seeking to take advantage of consumers by sending email phishing scams trying to have already concerned consumers provide important information to other thieves.

---

https://schakowsky.house.gov/uploads/Equifax.2017.09.12.Letter%20to%20Equifax%20CEO%20re%20consumer%20data%20breach.%20DCCP.OI.pdf (last accessed May 11, 2018).

[73] Jim Puzzaanghera, *Former Equifax CEO apologizes for data breach and details ways the company messed up*, LOS ANGELES TIMES (Oct. 2, 2017), http://www.latimes.com/business/la-fi-equifax-data-breach-20171002-story.html (last accessed May 11, 2018) ("Puzzaanghera, *Former Equifax CEO apologizes for data breach*").

150. Scammers were also able to successfully manipulate code on Equifax's website to prompt consumers to download a fraudulent update to Adobe Flash that installs adware, further exposing consumers' information.

151. Equifax also attempted to capitalize on the data breach by pushing its own data-protection services,[74] and initially charged many individuals to freeze their own credit files, which were at risk because of Equifax's own negligence.[75]

152. Many consumers who wanted to protect themselves after the breach, but did not want to utilize Equifax products, purchased products and services from "independent" companies like LifeLock, which reported a tenfold increase in enrollment during the month after the Equifax breach.[76] But under questioning, Richard Smith confirmed that LifeLock uses Equifax to monitor its customers' credit

---

[74] Yuki Noguchi, *After Equifax Hack, Consumers Are On Their Own. Here Are 6 Tips to Protect Your Data*, NATIONAL PUBLIC RADIO (Sept. 14, 2017), http://www.npr.org/2017/09/14/550949718/after-equifax-data-breach-consumers-are-largely-on-their-own (last accessed May 11, 2018) ("Noguchi, *After Equifax Hack, Consumers Are On Their Own*.").

[75] Ron Lieber, *Equifax, Bowing to Public Pressure, Drops Credit-Freeze Fees*, THE NEW YORK TIMES (Sept. 12, 2017), https://www.nytimes.com/2017/09/12/your-money/equifax-fee-waiver.html?rref=collection%2Fbyline%2Fron-lieber&action=click&contentCollection=undefined&region=stream&module=stream_unit&version=latest&contentPlacement=3&pgtype=collection (last accessed May 11, 2018).

[76] See Warren Report at 9.

and pays Equifax on a per customer basis for use of its services.[77] Thus, Equifax stood to *benefit* from the hundreds of thousands of new customers LifeLock received in the aftermath of the breach.[78]

153. Even worse, some Equifax executives sought to personally benefit by avoiding losses relating to the breach. On March 14, 2018, the Securities and Exchange Commission announced it had charged former Equifax CIO Jun Ying with insider trading.[79] The SEC alleged that Ying used insider information to discover that Equifax suffered a data breach, and then sold Equifax stock before the breach was publicly announced—avoiding approximately $117,000 in losses.[80]

---

[77] *Id*.

[78] Cory Doctorow, *Equifax will make hundreds of millions in extra profits from its apocalyptic breach (forever)*, BOING BOING (Oct. 5, 2017), https://boingboing.net/2017/10/05/failing-up-and-up.html (last accessed May 11, 2018).

[79] Renae Merle, *Former Equifax executive charged with illegally trading before massive data breach was made public*, THE WASHINGTON POST (Mar. 14, 2018), https://www.washingtonpost.com/news/business/wp/2018/03/14/former-equifax-executive-charged-with-insider-trading-ahead-of-data-breach/?utm_term=.cfb0c98b4ca2 (last accessed May 11, 2018).

[80] *Former Equifax Executive Charged With Insider Trading*, U.S. SECURITIES AND EXCHANGE COMMISSION (April 2018), https://www.sec.gov/news/press-release/2018-40 (last accessed May 11, 2018).

154. In September 2017, the FTC stated that it had begun investigating Equifax. Reporters noted that such a disclosure was unusual, as typically the FTC does not discuss open or ongoing investigations.[81]

155. On September 13, 2017, under the headline "Updated information on U.S. website application vulnerability," Equifax posted the following on its website: "Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. **The vulnerability was Apache Struts CVE-2017-5638.** We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement." (emphasis added).

156. Apache did not accept the blame, and responded that the breach "was due to [Equifax's] failure to install the security updates provided in a timely

[81] Brian Fung and Hamza Shaban, *The FTC is investigating the Equifax breach. Here's why that's a big deal.*, THE WASHINGTON POST (Sept. 14, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/14/the-ftc-confirms-its-investigating-the-equifax-breach-adding-to-a-chorus-of-official-criticism/?utm_term=.e5d4a0a2883a (last accessed May 11, 2018).

manner."[82] On September 15, 2017, Equifax updated its website, and acknowledged Apache's prior alert:

> Questions Regarding Apache Struts
>
> - The attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.
>
> - Based on the company's investigation, Equifax believes the unauthorized accesses to certain files containing personal information occurred from May 13 through July 30, 2017. The particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017.
>
> - Equifax's Security organization was aware of this vulnerability at that time, and took efforts to identify and to patch any vulnerable systems in the company's IT infrastructure.
>
> - While Equifax fully understands the intense focus on patching efforts, the company's review of the facts is still ongoing. The company will release additional information when available.

157. Since announcing the breach, Equifax has acknowledged on its website the problems relating to its public response to the breach that needed to be fixed, corrected, and clarified. According to the website, "since the announcement, Equifax has taken additional actions including:"

---

[82] Elizabeth Weise, et al., *Equifax had patch 2 months before hack and didn't install it, security group says*, USA TODAY (Sept. 14, 2017), https://www.usatoday.com/story/money/2017/09/14/equifax-identity-theft-hackers-apache-struts/665100001/ (last accessed May 11, 2018).

- Providing a more prominent and clear link from the main www.equifax.com website to the cybersecurity incident website www.equifaxsecurity2017.com, so that consumers can quickly and easily find the information they need.

- Tripling the call center team and continuing to add agents, despite facing some difficulty due to Hurricane Irma.

- Resolving issues with the impact look-up tool.

- Addressing confusion concerning the arbitration and class-action waiver clauses included in the Terms of Use applicable to the product.

- Because of consumer concern, the company clarified that those clauses do not apply to this cybersecurity incident or to the complimentary TrustedID Premier offering.

- The company clarified that the clauses will not apply to consumers who signed up before the language was removed.

- Clarifying that no credit card information is required to sign up for the product and that consumers will not be automatically enrolled or charged after the conclusion of the complimentary year.

- Making changes to address consumer concerns regarding security freezes.

- The company clarified that consumers placing a security freeze will be provided a randomly generated PIN.

- The company continues to work on technical difficulties related to the high volume of security freeze requests.

- Consumers who paid for a security freeze starting at 5pm EST on September 7, 2017 will receive a refund.

- The company agreed to waive fees for removing and placing security freezes through November 21, 2017.[83]

158. On September 26, 2017, Equifax announced that Richard Smith was stepping down as its CEO weeks before he was scheduled to testify before Congress. A New York Times article noted that Smith "presided over a period of rapidly growing sales [at Equifax], driven by expanding troves of sensitive personal data. Profits rose, and the stock price followed. When the crisis hit, the company stumbled. Its website repeatedly crashed as millions of desperate individuals tried to find out whether their information was part of the breach. People who were potentially affected were unable to sign up for protection the company was offering or, even if they had been successful, could not get the service activated. Equifax also charged many people to freeze their credit files before reversing course in the wake of fierce criticism."[84]

[83] https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832 (last accessed May 11, 2018).

[84] Ron Lieber and Stacy Cowley, *Trying to Stem Fallout From Breach, Equifax Replaces C.E.O.*, THE NEW YORK TIMES (Sept. 26, 2017), https://www.nytimes.com/2017/09/26/business/equifax-ceo.html (last accessed May 11, 2018).

159. Richard Smith was replaced by then-interim CEO, Paulino de Rego Barros Jr., who similarly acknowledged that "answers to key consumer questions were too often delayed, incomplete or both."[85]

160. Equifax also confirmed that its Chief Information Officer, Susan Mauldin, and Chief Security Officer, David Webb, were retiring "effective immediately."[86] As noted above, Ms. Mauldin has a bachelor's degree and a master of fine arts degree in music composition. After the breach, Equifax scrubbed its website of information relating to Ms. Mauldin.[87]

161. Equifax has also reportedly pointed fingers at its security consulting partner, Mandiant, claiming that, in the days after the breach, it "sent rookies to look into the vulnerabilities of its systems."[88] On October 2, 2017, Equifax announced that it had identified another 2.5 million people whose Personal Information was

---

[85] See Lieber, *How to Protect Yourself After the Equifax Breach*.

[86] Elizabeth Weise, *A timeline of events surrounding the Equifax data breach*, USA TODAY (Sept. 26, 2017), https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/ (last accessed May 11, 2018).

[87] Brett Arends, *Opinion: Equifax hired a music major as chief security officer and she has just retired*, MARKETWATCH (Sept. 15, 2017), http://www.marketwatch.com/amp/story/guid/766FA70C-9A38-11E7-B604-EDFD35AE15F2 (last accessed May 11, 2018).

[88] Jon Fingas, *Equifax breach shows signs of a possible state-sponsored hack*, YAHOO! FINANCE (Sept. 30, 2017), https://finance.yahoo.com/news/equifax-breach-shows-signs-possible-223100521.html (last accessed May 11, 2018).

compromised. The number of known victims increased from 143 million to 145.5 million.[89]

162. On October 3, 2017, former Equifax CEO Richard Smith testified before the House Digital Commerce and Consumer Protection subcommittee. In his testimony, Smith blamed the breach on an "individual" in its technology department who failed to implement the software fixes needed.[90] Apparently this individual "did not ensure communication got to the right person to manually patch the application."[91] Smith also testified that the scanning software Equifax employed to detect such vulnerabilities then also missed this error.[92]

163. Also in early October 2017, the Senate Committee on Banking, Housing and Urban Affairs, and the Senate Committee on the Judiciary, subcommittee on Privacy, Technology, and Law, held hearings regarding the Equifax data breach, at which Smith testified. Smith conceded that neither the

---

[89] Elizabeth Weise and Nathan Bomey, *Equifax breach hit 2.5 million more Americans than first believed*, USA TODAY (Oct. 2, 2017), https://www.usatoday.com/story/tech/2017/10/02/equifax-breach-hit-2-5-million-more-americans-than-first-believed/725100001/ (last accessed May 11, 2018).

[90] Tara Siegel Bernard and Stacy Cowley, *Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says*, THE NEW YORK TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html (last accessed May 11, 2018).

[91] *Id.*

[92] *Id.*

Apache Struts vulnerability nor its solution were "novel." He also conceded that fraud would increase after the breach.

164. On February 10, 2018, it was reported based on a document Equifax turned to Senate Banking Committee members that Equifax had "disclosed that tax identification numbers, email addresses and phone numbers" were also part of the breach, as well as issuing states for some driver's licenses and credit card expiration.[93]

165. On March 1, 2018, Equifax announced that 2.4 million more Americans were impacted by the data breach than previously disclosed.[94] These additional consumers had names and partial driver's license numbers stolen according to

[93] Donna Borak and Kathryn Vasel, *The Equifax hack could be worse than we thought*, CNN MONEY (Feb. 10, 2018), http://money.cnn.com/2018/02/09/pf/equifax-hack-senate-disclosure/index.html (last accessed May 11, 2018); *Equifax Breach Exposed More Consumer Data Than First Disclosed*, INSURANCE JOURNAL (Feb. 13, 2018), https://www.insurancejournal.com/news/national/2018/02/13/480357.htm (last accessed May 11, 2018); Craig Johnson, *Turns out, the Equifax data breach was even worse than we thought*, CLARK (Feb. 14, 2018), https://clark.com/consumer-issues-id-theft/identity-theft/equifax-data-breach-new-revelations-worse/ (last accessed May 11, 2018).

[94] Brian Fung, *Equifax's massive 2017 data breach keeps getting worse*, THE WASHINGTON POST (Mar. 1, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.65d30e38797b (last accessed May 11, 2018).

reports. It took approximately 300 days from the time of the breach to disclose the existence of these additional 2.4 million victims, and they have still not been individually notified.

166. And it was not until May 7, 2018, when Equifax filed an 8-K Form with the Securities and Exchange Commission, that Equifax finally revealed a full breakdown of the consumer information stolen in the breach.

Data Element Stolen	Standardized Columns Analyzed [1]	Approximate Number of Impacted U.S. Consumers
Name	First Name, Last Name, Middle Name, Suffix, Full Name	146.6 million
Date of Birth	D.O.B.	146.6 million
Social Security Number [2]	SSN	145.5 million
Address Information	Address, Address2, City, State, Zip	99 million
Gender	Gender	27.3 million
Phone Number	Phone, Phone2	20.3 million
Driver's License Number [3]	DL#	17.6 million
Email Address (w/o credentials)	Email Address	1.8 million
Payment Card Number and Expiration Date	CC Number, Exp Date	209,000
TaxID	TaxID	97,500
Driver's License State	DL License State	27,000

167. In all, over 147 million Americans had their Personal Information compromised, nearly all of whom had their name, address, date of birth, and Social Security number stolen as part of the breach.

Equifax Recommends Implementing Credit Freezes

168. The breach forced consumers to spend money to protect themselves, including purchasing products such as credit monitoring and "credit freezes." According to the FTC, a credit freeze, also known as a security freeze, allows a

consumer to restrict access to their credit report, which in turn makes it more difficult for identity thieves to open new accounts in that consumer's name.

169. While credit freezes can be effective in thwarting fraudulent activity, they are also costly, time-consuming, and can create barriers for consumers who are quickly in need of credit. For example, in order to institute a credit freeze, most consumers must pay a fee every time they want to freeze their credit, which can cost up to $10 per freeze depending on state law. If a consumer needs credit while under a credit freeze, she must first unfreeze her credit, again at a cost of up to $10 per unfreeze. The consumer then must pay again to have her credit frozen. Because credit freezes are most effective when they are implemented with all three major CRAs, consumers must pay Equifax, Experian, and TransUnion each time they want to freeze or unfreeze their credit. As Experian's website notes, "Those costs can add up."[95]

170. Credit freezes can also be challenging to implement given that CRAs are notoriously difficult to contact. As noted by a New York Times commenter in the aftermath of the Equifax breach, "Some people are waiting until the middle of

[95] Brian O'Connell, *7 Things You Need to Know Before Freezing Your Credit*, EXPERIAN BLOG (Sept. 20, 2017), https://www.experian.com/blogs/ask-experian/7-things-you-need-to-know-before-freezing-your-credit/ (last accessed May 11, 2018) ("O'Connell, *7 Things You Need to Know Before Freezing Your Credit*").

the night to try to use Equifax's security freeze website and even failing then to get through. It's like trying to get Bruce Springsteen tickets, except nobody wants to see this particular show."[96]

171. Additionally, the lag time associated with freezing and unfreezing credit can create problems when a consumer quickly needs credit, which can make it difficult for consumers to take out loans or make major purchases without planning days or weeks in advance. Experian's website acknowledges that, "Credit freezes can create delays and problems when credit is needed quickly in the case of applying for a loan, credit card, or even a job hunt. . . . During a freeze period, most companies will not extend credit until they check one's credit file with one or three major credit bureaus, and that takes time."[97]

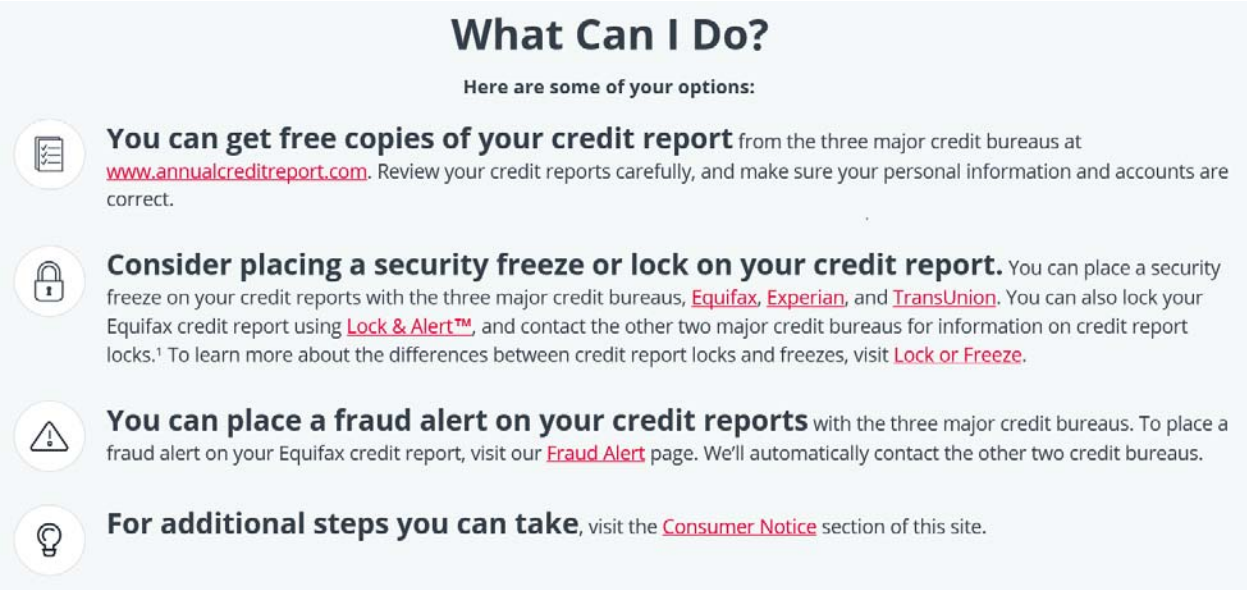
172. Although credit freezes are expensive and can be problematic for those seeking credit, they are among the best defenses to identity theft and fraud, and numerous consumer groups recommended that consumers freeze their credit in the aftermath of the breach. Given the scale of Personal Information compromised in

---

[96] Ron Lieber, *Finally, Some Answers From Equifax to Your Data Breach Questions*, THE NEW YORK TIMES (Sept. 14, 2017), https://www.nytimes.com/2017/09/14/your-money/equifax-answers-data-breach.html (last accessed May 11, 2018).

[97] See O'Connell, *7 Things You Need to Know Before Freezing Your Credit*.

the breach, Equifax itself recommended that consumers freeze their credit to mitigate possible harm in the aftermath of the breach, placing the following notice on its website:



What Can I Do?

Here are some of your options:

You can get free copies of your credit report from the three major credit bureaus at www.annualcreditreport.com. Review your credit reports carefully, and make sure your personal information and accounts are correct.

Consider placing a security freeze or lock on your credit report. You can place a security freeze on your credit reports with the three major credit bureaus, Equifax, Experian, and TransUnion. You can also lock your Equifax credit report using Lock & Alert™, and contact the other two major credit bureaus for information on credit report locks.[1] To learn more about the differences between credit report locks and freezes, visit Lock or Freeze.

You can place a fraud alert on your credit reports with the three major credit bureaus. To place a fraud alert on your Equifax credit report, visit our Fraud Alert page. We'll automatically contact the other two credit bureaus.

For additional steps you can take, visit the Consumer Notice section of this site.

173. While Equifax agreed to waive fees for implementing credit freezes for a limited period of time (after initially failing to do so), Experian and TransUnion continued to charge consumers full price for the privilege of freezing and unfreezing their credit after the breach.

174. As reported by Krebs on Security, almost 20 percent of Americans froze their credit file as a result of the Equifax breach, costing consumers an

estimated $1.4 billion. A survey conducted by Wakefield Research found that the average cost to consumers who froze their credit was $23.00.[98]

175. On May 9, 2018, Krebs on Security reported that some consumers were still reporting instances of identity theft relating to fraudulent mobile phone accounts being opened in their names, even after implementing credit freezes with the major three CRAs. This type of fraud was possible because many mobile phone merchants do not utilize Equifax, Experian, and TransUnion to process their credit inquiries, but instead they use a relatively obscure CRA known as the National Consumer Telecommunications and Utilities Exchange ("NCTUE").[99]

176. As explained by Krebs, "the NCTUE is a consumer reporting agency founded by AT&T in 1997 that maintains data such as payment and account history, reported by telecommunication, pay TV and utility service providers that are members of NCTUE."[100] After further investigation, Krebs determined that the

---

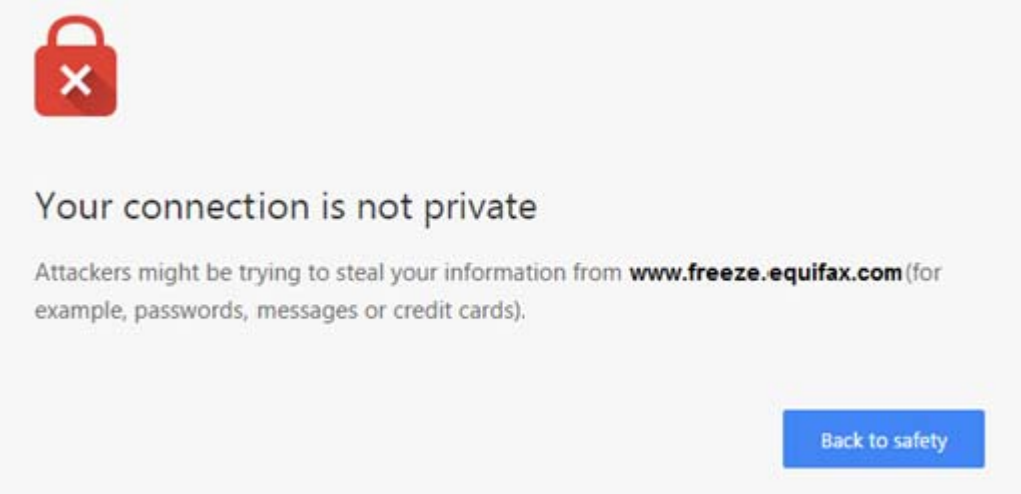
[98] Brian Krebs, *Survey: Americans Spent $1.4B on Credit Freeze Fees in Wake of Equifax Breac*h, KREBS ON SECURITY (Mar. 22, 2018), https://krebsonsecurity.com/2018/03/survey-americans-spent-1-4b-on-credit-freeze-fees-in-wake-of-equifax-breach/ (last accessed May 11, 2018).

[99] Brian Krebs, *Think You've Got Your Credit Freezes Covered? Think Again*, KREBS ON SECURITY (May 9, 2018), https://krebsonsecurity.com/2018/05/another-credit-freeze-target-nctue-com/ (last accessed May 11, 2018).

[100] *Id*.

NCTUE's website is hosted out of Equifax's servers, and Equifax is the sole contractor managing the NCTUE database.[101]

177. As part of his investigation, Krebs visited Equifax's credit freeze application webpage and realized it was using expired SSL certificates (an ongoing problem at Equifax), meaning that users visiting the webpage received a warning that attackers may be able to steal their information by accessing the website. A standard warning of this type appears below:



178. When Krebs visited the NCTUE webpage, he received the same warning. Consequently, not only has Equifax failed to correct its inadequate data security practices post-breach, it also likely dissuaded consumers from taking

[101] *Id.*

advantage of Equifax's (temporarily) free credit freezes for a number of weeks given that they were instructed not to access the website.[102]

179. The problem Equifax's relationship with NCTUE creates is obvious: "Many people who have succeeded in freezing their credit files with Equifax have nonetheless had their identities stolen and new accounts opened in their names thanks to a lesser-known credit bureau that seems to rely entirely on credit checking entities operated by Equifax."[103] Consequently, "Americans are in many cases plunking down $3-$10 per bureau to freeze their credit files, and yet a huge player in this market is able to continue to profit off of identity theft on those same Americans."[104]

180. Equifax attempted to explain away the apparent conflict by issuing a statement that the NCTUE is a separate entity, and the NCTUE does not include credit information from Equifax. But as noted above, Equifax listed the NCTUE as one of its primary "assets" in its 2009 Annual Report.

181. Indeed, in its press release regarding the breach, Equifax expressly referred to the NCTUE as one of its "core" databases, stating that "we have found

---

[102] *Id.*

[103] *Id.*

[104] *Id.*

no evidence that this cybersecurity incident impacted *Equifax's core consumer or commercial credit reporting databases*, including, ACRO, Workforce Solutions, including The Work Number payroll data, *NCTUE*, IXI and CFN." Equifax even sells a product known as "NCTUE Plus", which combines the NCTUE database with Equifax's traditional consumer credit database.[105]

182. Notwithstanding Equifax's attempt to distance itself from another controversy, this report adds to the mounting evidence that Equifax continues to capitalize on and benefit from the breach, while consumers are left with little to no recourse.

Reactions to the Data Breach

183. Reactions to the breach from industry analysts and Congressional members highlight its severity and adverse impact on a significant portion of the U.S. population. Avivah Litam, a fraud analyst at leading information technology consulting and research firm, Gartner, Inc., describing the Equifax breach, said, "[o]n a scale of 1-to 10 in terms of risk to consumers, this a 10."[106]

---

[105] https://www.equifax.com/business/nctue-plus/ (last accessed May 11, 2018).

[106] Tara Siegel Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, THE NEW YORK TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=3 (last accessed May 11, 2018) ("Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*").

184. Senator Mark Warner of Virginia stated, "It is no exaggeration to suggest that a breach such as this—exposing highly sensitive Personal Information central for identity management and access to credit—represents a real threat to the economic security of Americans."[107]

185. Massachusetts Attorney General Maura Healey called the Equifax data breach "the most brazen failure to protect consumer data we have ever seen."[108] Another commenter noted that the Equifax breach "will go down as one of the worst data breaches in history, and could prove to be the most damaging ever for American consumers."[109]

186. In February 2018, Equifax was ranked as the No. 1 "Most Hated Company in America", beating out dozens of bad reputation challengers including the NFL (No. 3), Wells Fargo (No. 11), Comcast (No. 15), Monsanto (No. 16) and The Weinstein Company (No. 20).[110]

---

[107] Craig Timberg, et al., *Data of 143 million Americans—nearly half the country—exposed in Equifax hack*, CHICAGO TRIBUNE (Sept. 8, 2017), http://www.chicagotribune.com/business/national/ct-equifax-data-breach-20170907-story.html (last accessed May 11, 2018).

[108] See Noguchi, *After Equifax Hack, Consumers Are On Their Own.*

[109] *Equifax breach could be worst in history*, SCOTSMAN GUIDE (Sept. 11, 2017), https://www.scotsmanguide.com/News/2017/09/Equifax-breach-could-be-worst-in-history/ (last accessed May 11, 2018).

[110] Samuel Stebbins, et al., *Bad reputation: America's Top 20 most-hated companies*, USA TODAY (Feb. 12, 2018),

187. In written testimony for his hearing with the House Energy and Commerce Committee, former Equifax CEO Richard Smith stated, "Equifax was entrusted with Americans' private data and we let them down," acknowledged the "human error" involved, and said that "[t]he company failed to prevent sensitive information from falling into the hands of wrongdoers."[111]

188. Perhaps most significantly, consumers have no way of "opting out" of Equifax's data collection or hindering Equifax's ability to profit from the sale of such information.[112] During his testimony before the United States Senate, Equifax's former CEO testified that he did not think that people should be able to delete their data from Equifax's systems.[113]

189. As referenced above, in February 2018, Senator Elizabeth Warren's office released a 15-page report summarizing its findings after a multi-month investigation that included questioning Equifax executives in Senate hearings, consulting outside experts, and sending letters containing dozens of questions to

---

https://www.usatoday.com/story/money/business/2018/02/01/bad-reputation-americas-top-20-most-hated-companies/1058718001/ (last accessed May 11, 2018).

[111] See Puzzaanghera, *Former Equifax CEO apologizes for data breach*.

[112] Ron Lieber, *'Dear Equifax: You're Fired.' If Only It Were That Easy.*, THE NEW YORK TIMES (Oct. 6, 2017), https://www.nytimes.com/2017/10/06/your-money/credit-scores/equifax-hack.html (last accessed May 11, 2018).

[113] *Id*.

Equifax, federal regulators, and other credit rating agencies. In addition to the findings summarized above relating to Equifax's inadequate data security practices, the Warren Report concluded that:

a. ***Equifax Set up a Flawed System to Prevent and Mitigate Data Security Problems***. The breach was made possible because Equifax adopted weak cybersecurity measures that did not adequately protect consumer data. The company failed to prioritize cybersecurity and failed to follow basic procedures that would have prevented or mitigated the impact of the breach. For example, Equifax was warned of the vulnerability in the web application software Apache Struts that was used to breach its system, and emailed staff to tell them to fix the vulnerability—but then failed to confirm that the fixes were made. Subsequent scans only evaluated part of Equifax's system and failed to identify that the Apache Struts vulnerability had not been remediated.

b. ***Equifax Ignored Numerous Warnings of Risks to Sensitive Data***. Equifax had ample warning of weaknesses and risks to its systems. Equifax received a specific warning from the Department of Homeland Security about the precise vulnerability that hackers took advantage of to breach the company's systems. The company had been subject to several smaller breaches in the years prior to the massive 2017 breach, and several outside experts identified and reported weaknesses in Equifax's cyber defenses before the breach occurred. But the company failed to heed—or was unable to effectively heed—these warnings.

c. ***Equifax Failed to Notify Consumers, Investors, and Regulators about the Breach in a Timely and Appropriate Fashion***. The breach occurred on May 13, 2017, and Equifax first observed suspicious signs of a problem on July 29, 2017. But Equifax failed to notify consumers, investors, business partners, and the appropriate regulators until 40 days after the company discovered the breach. By failing to provide adequate information in a timely fashion, Equifax robbed consumers of the ability to take precautionary measures to protect themselves, materially injured investors and withheld market-moving information,

and prevented federal and state governments from taking action to mitigate the impacts of the breach.

d. ***Equifax Took Advantage of Federal Contracting Loopholes and Failed to Adequately Protect Sensitive IRS Taxpayer Data***. Soon after the breach was announced, Equifax and the IRS were engulfed in controversy amid news that the IRS was signing a new $7.2 million contract with the company. Senator Warren's investigation revealed that Equifax used contracting loopholes to force the IRS into signing this "bridge" contract, and the contract was finally cancelled weeks later by the IRS after the agency learned of additional weaknesses in Equifax security that potentially endangered taxpayer data.

e. ***Equifax's Assistance and Information Provided to Consumers Following the Breach was Inadequate***. Equifax took 40 days to prepare a response for the public before finally announcing the extent of the breach—and even after this delay, the company failed to respond appropriately. Equifax had an inadequate crisis management plan and failed to follow their own procedures for notifying consumers. Consumers who called the Equifax call center had hours-long waits. The website set up by Equifax to assist consumers was initially unable to give individuals clarity other than to tell them that their information "may" have been hacked—and that website had a host of security problems in its own right. Equifax delayed their public notice in part because the company spent almost two weeks trying to determine precisely which consumers were affected by the breach—but then failed to provide consumers with any specific information to determine if their data was breached. And while Equifax continues to publicly state only that data was "accessed," the company has confirmed that the data was exfiltrated—stolen—from their systems and downloaded by the hackers. Equifax appeared to be more focused on using the breach as a profitmaking opportunity for other company services rather than providing redress to consumers.[114]

[114] See Warren Report at 2.

The Warren Report concluded that "Equifax and other credit reporting agencies have taken advantage of consumers for years, collecting their data without permission and turning a huge profit while failing to adequately protect that data." The report recommended that federal legislation be enacted to force "Equifax and its peers to put appropriate emphasis on protecting consumer data."[115]

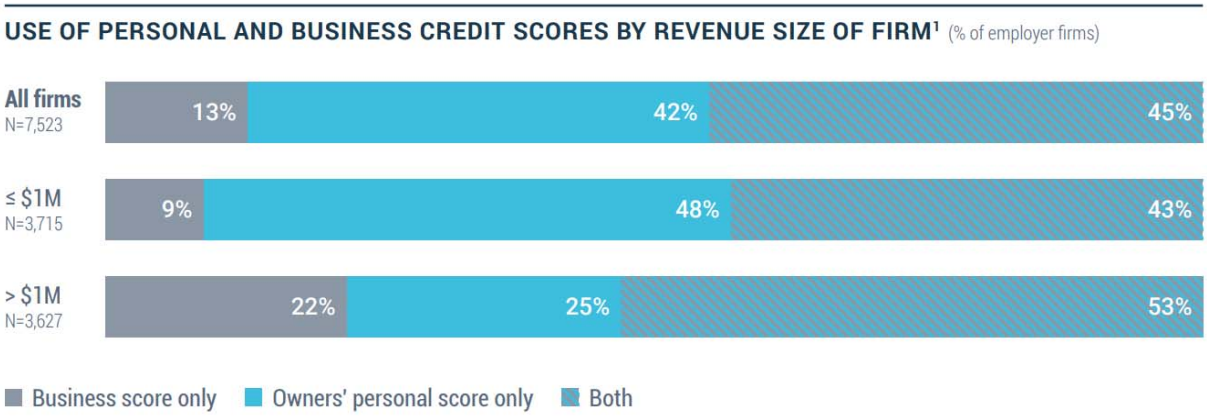
Aftermath of the Breach: Consequences for Small Businesses

190. Most U.S. businesses use credit to fund their operations, and their ability to obtain and use credit is often tied to the business owners' personal credit.

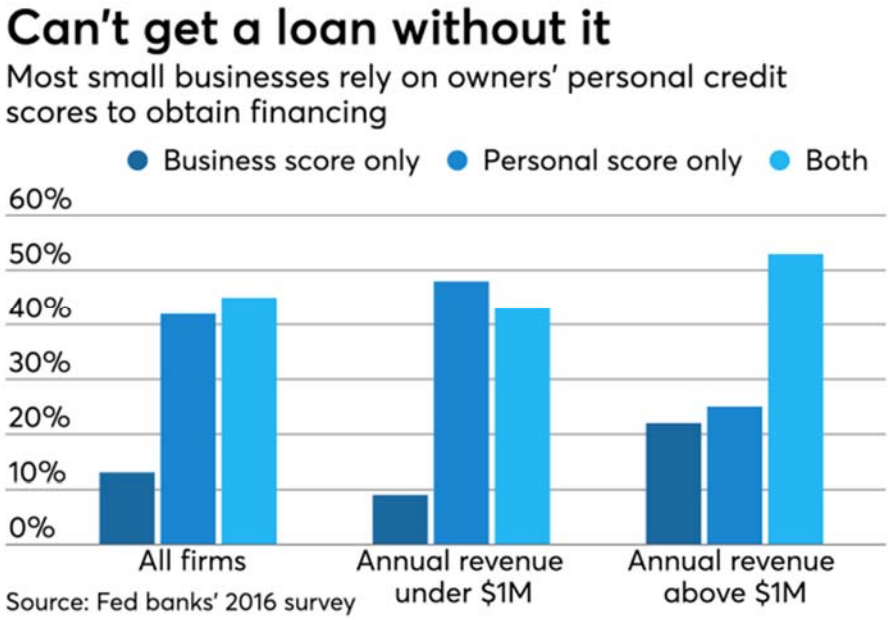
191. According to a 2016 Federal Reserve survey, 87% of small businesses in the United States rely on their owners' personal credit scores (either alone or in tandem with a business credit score) to maintain financing.[116]

[115] *Id*. at 11.

[116] Kevin Wack, *Equifax breach threatens small businesses, too*, AMERICAN BANKER (Sept. 27, 2017), https://www.americanbanker.com/news/equifax-breach-threatens-small-businesses-too.



192. Firms with $1 million or less in annual revenue depend at least in part on owners' personal credit scores in about 91% of instances. The below graph[117] reflects these numbers:



[117] *Id.*

193. The same survey concluded that 87 percent of small businesses use personal guarantees to secure outstanding debts.[118]

194. With small businesses so heavily dependent on their owners' personal credit, the Equifax breach, and the resulting damage and jeopardy to personal creditworthiness, poses severe risks to small businesses. The breach has jeopardized their businesses' access to credit and the price they pay for credit, and thus also their operations, collateral, and viability.

195. On September 26, 2017, the ranking members of the Senate Committee on Small Business & Entrepreneurship and the House Committee on Small Business wrote a letter to the chairman of Equifax about "the significant potential exposure of small businesses as a result of this breach."[119] The letter emphasizes the fact that the "availability of business credit for small business owners is inextricably tied to their personal credit score," and the authors wrote that they were "gravely concerned

---

[118] Small Business Credit Survey, Report on Employer Firms (Apr. 2017), *available at* https://www.newyorkfed.org/medialibrary/media/smallbusiness/2016/SBCS-Report-EmployerFirms-2016.pdf.

[119] Sept. 26, 2017 Ltr. to Mark Feidler and Paulino do Rego Barros, Jr. from Sen. Jeanne Shaheen and Rep. Nydia Velázquez, *available at* https://democrats-smallbusiness.house.gov/sites/democrats.smallbusiness.house.gov/files/Letter%20from%20Senator%20Shaheen%20and%20Congresswoman%20Velazquez%20to%20Equifax%20-%20September%2026%202017.pdf

about the effect this breach will have on the ability of small businesses to access affordable credit."

196. The authors wrote that they were "concerned about the impact of the historic cybersecurity breach at Equifax will have on our country's 29 million small business owners." The letter explains that the Equifax breach will likely cause businesses to be offered "less favorable terms, including higher interest rates or outright denial" of credit, which will "squeeze cash flow, hurt their bottom line, and jeopardize their . . . collateral."

197. In a statement accompanying the letter, Senator Jeanne Shaheen said, "This [breach] could be devastating for these businesses and their ability to get credit on reasonable terms. Equifax has an obligation to make this right."[120]

198. A *CNN Money* article similarly recognized that identity theft resulting from the Equifax breach is likely to harm businesses by leading to "higher interest rates or outright rejection of . . . loan application[s]," jeopardizing the continued viability of the businesses.[121] The same article quotes Molly Day, Vice President of

[120] Shaheen to Equifax: Provide Assistance to Small Businesses Caught up in Data Breach (Sept. 27, 2017), https://www.shaheen.senate.gov/news/press/shaheen-to-equifax-provide-assistance-to-small-businesses-caught-up-in-data-breach.

[121] Katie Lobosco, *Why the Equifax hack has small business owners worried*, CNN (Sept. 28, 2017), http://money.cnn.com/2017/09/28/pf/equifax-small-business-lawsuit/index.html.

Public Affairs at the National Small Business Association: "You could be running your business just fine and still have trouble accessing credit. That's why things like this hack can be so worrisome."

199. Another financial blog noted, "business owners face far greater risks in the event their credit information is compromised. For instance, if a new application for credit is denied due to a poor personal credit history based on fraudulent accounts, a business may be unable to make payroll, cover overhead expenses, or affordably finance an expansion. Additionally, signing a new lease for commercial space may be a challenge if personal credit is tarnished. There may also be negative tax consequences if a delinquent, fraudulent account finds its way to collections, harming the business even further. Each of these consequences of stolen personal information has a vast impact on small business owners."[122]

200. An article by *American Banker* (a media outlet that directs information to executives in the financial services industry) concurred with the assessment that the breach harms U.S. businesses. That article explains how the breach leaves millions of businesses all "in the same predicament," jeopardizing both the owner's

[122] APR Finder, How the Equifax Data Breach Affects Business Credit, *available at* https://www.aprfinder.com/equifax-data-breach-business-credit-affect.

and business's credit.[123] The article quotes Adrian Nazari, the CEO of Credit Sesame, a website that offers free credit scores to consumers: "The majority of businesses in America are sole proprietor businesses, and the line between business and personal credit is very blurry." The article notes the general lack of clarity about "what steps business owners should take to best protect themselves," and emphasized business credit monitoring services as a viable option.

201. Equifax has itself acknowledged that the credit histories of business owners are "an essential element" for understanding businesses' credit risks.[124]

202. Equifax markets business credit reports as a product analogous to consumer credit reports, and the business credit reports provide information on the businesses' owners and guarantors,[125] for the "deepest level of insight into the validity, financial stability and performance" of the business.[126]

---

[123] *See* Wack, *Equifax breach threatens small businesses, too*.

[124] Equifax White Paper, *Mastering the Small-Business Market: A Guide to Understanding 4 Critical Credit Risk Trends* (March 6, 2013) (available at https://www.equifax.com/commercialsolutions/nacs/documents/Risk_SMB_Insights_Brief-Mastering_the_SMB_Market.pdf).

[125] *Training Guide Business Credit Industry Report Plus 2.0* (August 31, 2012) (available at https://assets.equifax.com/assets/nacs/efx-2036_bcir_plus_2-0.pdf).

[126] Equifax Business Credit Reports, https://www.equifax.com/business/business-credit-reports/.

203. After the breach, Equifax introduced a product that it markets as the "first [credit monitoring] solution to combine consumer credit information with . . . business credit data."[127] In a press release for the product, an Equifax Senior Vice President said, "Providing our customers with the option of combining consumer data and small business data . . . will redefine the US Commercial Risk Management market."

204. In marketing a product that Equifax calls the "Business Principal Report," Equifax acknowledges that to "understand the potential risk associated with a business, particularly small businesses and sole proprietorships, it's important to also understand the business owners and principal guarantors and their relevant business associations and financial issues."[128] Equifax markets the product as capable of providing "comprehensive information about the credit history of a business principal, plus you are alerted to potentially fraudulent information about the individual that might require further verification, and whether the individual has a higher potential for late payments." Equifax also markets the ability to "[l]everage

[127] *Equifax Blends Consumer and Commercial Data to Deliver Substantial Small Business Risk Prediction* (Apr. 24, 2018), https://investor.equifax.com/news-and-events/news/2018/04-24-2018-140548353.

[128] Equifax Business Principal Report, https://www.equifax.com/business/business-principal-report/.

public records, credit and business owner data from Equifax and other third-party providers" to assess a business's creditworthiness.[129]

205. Equifax also sells a product called "business risk scores," which Equifax markets as facilitating "smart, efficient credit decisions" and providing "reliable insight into fraud and financial risk, general credit worthiness and potential for failure."[130]

206. Following the Equifax breach, many have said it is "essential" that businesses actively monitor their credit, including by paying for credit monitoring and related services such as those listed above.[131]

207. The September 2017 letter from the ranking members of the Senate Committee on Small Business & Entrepreneurship and the House Committee on Small Business to Equifax, for example, notes that "identity theft is especially devastating" for small business owners especially because various legal and practical protections that benefit individuals are not available for businesses. The letter's

---

[129] Equifax White Paper, *Lennox Transforms Credit and Collections with Help of Dynamic Equifax Solution*, https://assets.equifax.com/assets/nacs/business_connect_lennox_cs.pdf.

[130] Equifax Business Risk Scores, https://www.equifax.com/business/business-risk-scores/.

[131] *E.g.*, *The Equifax Breach Can Impact your Business & Personal Credit*, North Shore Advisory, Inc. Credit Experts, https://northshoreadvisory.com/blog/equifax-breach-protect-personal-business-credit/.

authors thus urged Equifax to provide "protective products" specific to businesses and to recognize that "just as the credit needs of small businesses differ from consumers, the solutions and protections for small businesses need to be different in responding to and mitigating the impact of identity theft."

208. The September 2017 letter from the ranking members of the Senate Committee on Small Business & Entrepreneurship and the House Committee on Small Business to Equifax asked Equifax to provide relief and assistance to businesses. Equifax never responded, however, and has refused to provide relief to America's small businesses.

209. Unlike consumers, who are entitled under federal law to obtain one free credit report annually, businesses must pay for their credit reports. Despite the risks to businesses that Equifax caused through its negligence and the resulting breach, and despite the Congressional request that Equifax provide businesses with some form of relief, Equifax continues to charge businesses $99.99 for a single credit report. Other companies likewise charge for business credit reports. For example, Experian charges between $39.95 per business credit report and $149 annually for a Business Credit Advantage plan.

210. As a credit bureau that determines the creditworthiness of individuals and businesses and that also sells financial products to prevent business identity

theft, it was foreseeable to Equifax that its carelessness in the protection of consumer data would jeopardize the credit and operations of small businesses around the country and would spur them to spend money on business credit monitoring and other such credit products that they would not otherwise purchase.

211. In the aftermath of the breach, Equifax has elected to profit from its misconduct rather than voluntarily help small businesses. Equifax continues to charge businesses for credit monitoring and protection products. Thus, even though Equifax's negligence is what jeopardized the credit and operations of America's small businesses, Equifax is now charging those businesses to guard against the very risks that Equifax created.

CLASS ACTION ALLEGATIONS

212. Pursuant to Fed. R. Civ. P. 23(b)(3) and (c)(4), Business Plaintiffs assert common law claims for negligence (Count 1), negligence *per se* (Count 2), violations of the Georgia Fair Business Practices Act (Count 3), and unjust enrichment (Count 4) on behalf of themselves and the following nationwide class (the "Nationwide Class" or the "Class"):

NATIONWIDE CLASS

All businesses in the United States that have relied on an owner's personal credit to obtain or maintain financing between September 7, 2017, and the present, which owner's Personal Information was compromised as a result of the data breach announced by Equifax on or about September 7, 2017, as identified by Equifax's records relating to that data breach.

213. In the alternative, pursuant to Fed. R. Civ. P. 23(b)(3) and (c)(4), Business Plaintiffs assert state-wide subclasses on behalf of businesses in each of their respective states.

214. Excluded from the Nationwide Class and each Subclass, if applicable, are Equifax, any entity in which Equifax has a controlling interest, and Equifax's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each Subclass are any judicial officers presiding over this matter, members of their immediate family, and members of their judicial staff. Also excluded from the Nationwide Class and each Subclass are all banks, credit unions, and financial institutions, as well as all natural persons, and those individuals who are included in the class definitions in the Consolidated Consumer Class Action Complaint, filed on May 14, 2018.

215. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. There are approximately

29 million small businesses in the United States, the vast majority of which obtain credit by relying (in whole or in part) on the business owner's personal credit worthiness. There are several administratively feasible methods by which these businesses can be identified: Their names and addresses are available from Equifax's records, including Equifax's business credit report data, which list business names, addresses, and owner and guarantor information; alternatively, Class members can self-identify and provide their credit documentation to confirm their Class membership. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, Internet postings, and/or published notice.

216. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3)**. As to each Class and Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual class members, including, without limitation:

a. Whether Equifax knew or should have known that its computer systems were vulnerable to attack;

b. Whether Equifax failed to take adequate and reasonable measures to ensure its data systems were protected;

c. Whether Equifax failed to take available steps to prevent and stop the breach from happening;

d. Whether Equifax owed a duty to Business Plaintiffs and Class and Subclass members to protect Personal Information;

e. Whether Equifax breached its duties to protect Personal Information by failing to provide adequate data security;

f. Whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unauthorized access and/or theft of tens of millions of consumers' Personal Information;

g. Whether Equifax's conduct renders it liable for negligence, negligence *per se*, unjust enrichment, or under the Georgia Fair Business Practices Act; and

h. Whether, as a result of Equifax's conduct, Business Plaintiffs and Class and Subclass members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

i. Whether, as a result of Equifax's conduct, Business Plaintiffs and Class and Subclass members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

217. **Typicality: Federal Rule of Civil Procedure 23(a)(3)**. As to each Class and Subclass, Business Plaintiffs' claims are typical of other Class members' claims because Business Plaintiffs and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

218. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4)**. Business Plaintiffs are adequate class representatives because their interests do not conflict with the interests of Class members who they seek to represent, Business Plaintiffs have retained counsel competent and experienced in complex class action litigation, and Business Plaintiffs intend to prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Business Plaintiffs and their counsel.

219. **Superiority: Federal Rule of Civil Procedure 23(b)(3)**. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Business Plaintiffs and Class members are relatively small compared to the

burden and expense that would be required to individually litigate their claims against Equifax, so it would be impracticable for Class members to individually seek redress for Equifax's wrongful conduct. Even if Class members could afford litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CHOICE OF LAW FOR NATIONWIDE CLAIMS

220. The State of Georgia has a significant interest in regulating the conduct of businesses operating within its borders. Georgia, which seeks to protect the rights and interests of Georgia and all residents and citizens of the United States against a company headquartered and doing business in Georgia, has a greater interest in the nationwide claims of Plaintiffs and Nationwide Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

221. The principal place of business of Equifax, located at 1550 Peachtree Street NE, Atlanta, Georgia, is the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's

activities, including its data security functions and major policy, financial, and legal decisions.

222. Equifax's response to the data breach at issue here, and corporate decisions surrounding such response, were made from and in Georgia.

223. Equifax's breaches of duty to Plaintiffs and Nationwide Class members emanated from Georgia.

224. Application of Georgia law to the Nationwide Class with respect to Plaintiffs' and Class members' claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Nationwide Class.

225. Under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia applies to the nationwide common law claims of all Nationwide Class members. Additionally, given Georgia's significant interest in regulating the conduct of businesses operating within its borders, Georgia's Fair Business Practices Act may be applied to non-resident small business plaintiffs.

CAUSES OF ACTION

COUNT 1
NEGLIGENCE

On Behalf of Business Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Business Plaintiffs and any applicable Statewide Subclasses

226. Business Plaintiffs repeat and reallege Paragraphs 1-225, as if fully alleged herein.

227. Equifax knew that Small Business Plaintiffs and Class Members were directly affected by the security of Personal Information controlled by Equifax. Equifax owed a duty to Business Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting that Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Equifax's security systems to ensure that this Personal Information in Equifax's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

228. Equifax's duty to use reasonable care arose from several sources, including but not limited to those described below.

229. Equifax had a common law duty to prevent foreseeable harm to others. This duty existed because Business Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Business Plaintiffs and Class Members would be harmed by the failure to protect Personal Information in Equifax's control because hackers routinely attempt to steal such information and use it for nefarious purposes, Equifax knew that it was more likely than not Business Plaintiffs and other Class members would be harmed.

230. Equifax's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Equifax. Various FTC publications and data security breach orders further form the basis of Equifax's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

231. Equifax's duty also arose from Equifax's unique position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. Equifax undertakes its collection of highly sensitive information generally without the knowledge or consent of consumers and consumers cannot "opt out" of Equifax's data collection activities. Equifax holds itself out as a trusted steward of consumer data, and thereby assumes a duty to reasonably protect that data. The consumer public and, indeed, all those who participate in modern American economic life collectively repose a trust and confidence in Equifax to perform that stewardship carefully. Otherwise consumers would be powerless to fully protect their interests with regard to their Personal Information, which is controlled by Equifax. Because of its crucial role within the credit system, Equifax was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class members as a result of the Equifax data breach.

232. Equifax admits that it has an enormous responsibility to protect sensitive personal and financial data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the Personal Information at issue here.

233. Equifax's duty also is based on the FCRA, which reflects Congress's considered judgment that CRAs such as Equifax hold a unique and superior position in our credit economy, a position that if abused would foreseeably and probably

injure Business Plaintiffs and Class members. The FCRA thus requires that Equifax maintain reasonable procedures designed to avoid unauthorized release of information contained in consumer reports, and requires that when issued, consumer reports are complete and accurate.

234. Equifax also acknowledges and recognizes a pre-existing duty to exercise reasonable care to safeguard Personal Information that extends to those who are entrusted with such information. When dealing with businesses that purchase consumer information from Equifax, Equifax explicitly recognizes and contractually insists that those businesses have a duty to protect this information. For example, in its form Broker Subscription Agreement, Equifax requires that:

- "only Authorized Users can order or have access to" protected information;
- credit reports are not provided "to any third party except as permitted";
- protected information "must be encrypted when not in use and all printed [protected information] must be stored in a secure, locked container when not in use, and must be completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose";

- protected information must be encrypted with: "Advanced Encryption Standard (AES), minimum 128-bit key or Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms";
- Equifax's business partner must "monitor compliance" with these obligations "and immediately notify EQUIFAX if [the business partner] suspects or knows of any unauthorized access or attempt to access the" protected information;
- Equifax's business partner must "not ship hardware or software . . . to third parties without deleting . . . any consumer information";
- Equifax's business partner must "use commercially reasonable efforts to assure data security when disposing or any consumer report information";
- "Such efforts must include the use of those procedures issued by" applicable federal agencies, "e.g. the Federal Trade Commission . . . ."

235. With regard to network security, Equifax further acknowledges and requires that its business partners must "use commercially reasonable efforts to protect EQUIFAX Information when stored on servers, subject to the following requirements":

- "EQUIFAX Information must be protected by multiple layers of network security, including but not limited to, firewalls, routers, intrusion detection device";
- "secure access (both physical and network) to systems storing EQUIFAX Information must include authentication and passwords that are changed at least every 90 days";
- "all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available."

236. Equifax also had a duty to safeguard the Personal Information of Business Plaintiffs and Class members and to promptly notify them of a breach because of various state laws and statutes that require Equifax to reasonably safeguard sensitive Personal Information.

237. Timely notification was required, appropriate and necessary so that, among other things, Business Plaintiffs and Class members could take appropriate measures to freeze or lock credit profiles, avoid unauthorized charges to credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor account information and credit reports for fraudulent activity, contact banks or other financial institutions that issue credit or debit cards, obtain

business credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Equifax's misconduct.

238. Equifax breached the duties it owed to Business Plaintiffs and Class members described above and thus was negligent. Equifax breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect Personal Information that directly affects Business Plaintiffs and Class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Personal Information in Equifax's possession had been or was reasonably believed to have been, stolen or compromised.

239. But for Equifax's wrongful and negligent breach of its duties owed to Business Plaintiffs and Class members, their Personal Information would not have been compromised.

240. As a direct and proximate result of Equifax's negligence, Business Plaintiffs and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT 2
NEGLIGENCE *PER SE*

On Behalf of Business Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Business Plaintiffs and any applicable Statewide Subclasses

241. Business Plaintiffs repeat and reallege Paragraphs 1-225, as if fully alleged herein.

242. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Equifax of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Equifax's duty.

243. Equifax violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with industry standards. Equifax's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach at one of the three major credit bureaus.

244. Equifax's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

245. Class members are within the class of whom Section 5 of the FTC Act (and similar state statutes) was intended to protect. Section 5 bars unfair methods of competition and unfair and deceptive acts and practices "in or affecting commerce." Business Plaintiffs are engaged in commerce and their ability to obtain and maintain credit, as well as their ability to fund their operations and thus to continue to engage in commerce, was harmed by Equifax's misconduct and the breach. Moreover, virtually all Business Plaintiffs and Class members are owned and run by, and employ, consumers.

246. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Business Plaintiffs and the Class.

247. As a direct and proximate result of Equifax's negligent conduct, Business Plaintiffs and Class members have suffered injury as described above, and are entitled to damages including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT 3
GEORGIA FAIR BUSINESS PRACTICES ACT

On Behalf of Business Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and any applicable Statewide Subclasses

248. Business Plaintiffs repeat and allege Paragraphs 1-225, as if fully alleged herein.

249. The Georgia Fair Business Practices Act ("Georgia FBPA") provides that "[a]ny person who suffers injury or damages as a result of . . . consumer acts or practices in violation of [the FBPA] . . . may bring an action." O.C.G.A. § 10-1-399(a). The statute defines "person" to mean a "natural person, corporation, trust, partnership . . . or any other legal entity." Accordingly, Equifax, Business Plaintiffs, and Class members are "persons" within the meaning of the Georgia FBPA. O.C.G.A. § 10-1-399(a).

250. Equifax is engaged in, and its acts and omissions affect, trade and commerce under O.C.G.A. § 10-1-392(28). Further, Equifax is engaged in "consumer acts or practices," which are defined as "acts or practices intended to encourage consumer transactions" under O.C.G.A. §10-1-392(7). Equifax, in its capacity as a "consumer reporting agency," generates and maintains "consumer reports" and "files" subject to the GFBPA. O.C.G.A. §10-1-392 (9)-(10), (14).

251. Equifax's acts, practices, and omissions at issue in this matter were directed and emanated from its headquarters in Georgia.

252. Equifax engaged in "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce" in violation of O.C.G.A. § 10-1-393(a). Those acts and practices include those expressly declared unlawful by O.C.G.A. § 10-1-393(b), such as:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

253. In addition, Equifax engaged in the unfair and deceptive acts and practices described below that, while not expressly declared unlawful by O.C.G.A. § 10-1-393(b), are prohibited by O.C.G.A. § 10-1-393(a).

254. In the course of its business, Equifax engaged in unfair acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect the Personal Information at issue, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which were a direct and proximate cause of the Equifax data breach; and

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Personal Information at issue, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the Equifax data breach.

255. In the course of its business, Equifax also engaged in deceptive acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

a. Misrepresenting that it would protect the privacy and confidentiality of the Personal Information at issue, including by implementing and maintaining reasonable security measures;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of the Personal Information at issue, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq.;

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure the Personal Information at issue; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of the Personal Information at issue, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq.

256. The misrepresentations and omissions described in the preceding paragraph were material and made intentionally and knowingly with the intent that consumers, Business Plaintiffs, Class members, and others (such as its customers, data furnishers, regulators, investors, participants in the credit markets, and those who otherwise used data from Equifax for business purposes) rely upon them in

connection with accessing, storing, and using for business credit purposes the extremely sensitive and valuable Personal Information.

257. Equifax did all of this directly with respect to Business Plaintiffs and Class members, and also by way of their transactions involving goods, merchandise, and services with third parties (such as prospective creditors and creditors) who also accessed Business Plaintiffs' and Class members' sensitive and valuable Personal Information in the course of those transactions.

258. Additionally, after it learned of the breach, Equifax failed to notify the public of its existence for an unreasonable length of time. Worse, it continued to market credit monitoring and identity theft protection services, and even developed new products specifically targeted to Business Plaintiffs and Class members to take advantage of the breach and its negligent, unlawful, and unfair practices by charging those very same Business Plaintiffs and Class members for its products

259. Equifax did all of this directly with respect to consumers, Business Plaintiffs, and Class members, and also by way of their transactions involving goods, merchandise, and services with third parties (such as prospective creditors and creditors) who also accessed the Personal Information at issue in the course of those transactions.

260. Business Plaintiffs and Class members are entitled to a judgment against Equifax for actual and consequential damages, general and exemplary damages and attorneys' fees pursuant to the Georgia FBPA, costs, and such other further relief as the Court deems just and proper.

COUNT 4
UNJUST ENRICHMENT

On Behalf of Business Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and any applicable Statewide Subclasses

261. Business Plaintiffs repeat and allege Paragraphs 1-225, as if fully alleged herein.

262. Plaintiffs and Class members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Equifax and that was ultimately stolen in the Equifax data breach. This Personal Information was conferred on Equifax in most cases by third-parties but in some instances directly by Plaintiffs and Class members themselves.

263. Equifax was benefitted by the conferral upon it of the Personal Information pertaining to Plaintiffs and Class members and by its ability to retain and use that information. Equifax understood that it was in fact so benefitted.

264. Equifax also understood and appreciated that the Personal Information pertaining to Plaintiffs and Class members was private and confidential and its value

depended upon Equifax maintaining the privacy and confidentiality of that Personal Information.

265. But for Equifax's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted with Equifax. Further, if Equifax had disclosed that its data security measures were inadequate, Equifax would not have been permitted to continue in operation by regulators, its shareholders, and participants in the marketplace.

266. As a result of Equifax's wrongful conduct as alleged in this Complaint (including among things its utter failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiffs and Class members without having adequate data security measures, and its other conduct facilitating the theft of that Personal Information), Equifax has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class members. Among other things, Equifax continues to benefit and profit from the sale of the Personal Information while its value to Plaintiffs and Class members has been diminished.

267. Equifax's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive Personal Information, while at the same

time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

268. Under the common law doctrine of unjust enrichment, it is inequitable for Equifax to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and Class members in an unfair and unconscionable manner. Equifax's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

269. The benefit conferred upon, received, and enjoyed by Equifax was not conferred officiously or gratuitously, and it would be inequitable and unjust for Equifax to retain the benefit.

270. Equifax is therefore liable to Plaintiffs and Class members for restitution in the amount of the benefit conferred on Equifax as a result of its wrongful conduct, including specifically the value to Equifax of the Personal Information that was stolen in the Equifax data breach and the profits Equifax is receiving from the use and sale of that information

RECOVERY OF EXPENSES OF LITIGATION ON BEHALF OF ALL BUSINESS PLAINTIFFS

COUNT 5
O.C.G.A. § 13-6-11

271. Pursuant to O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense."

272. Defendants through their actions alleged and described herein acted in bad faith with respect to the transaction or events underlying this litigation.

273. Business Plaintiffs therefore request that their claim for recovery of expenses of litigation be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

REQUEST FOR RELIEF

Business Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Equifax, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare

that Business Plaintiffs are proper class representatives; and appoint Business Plaintiffs' Co-Lead and Co-Liaison Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Equifax from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Business Plaintiffs and Class members all available monetary relief, including compensatory, consequential, and general damages in an amount to be determined at trial;

4. That the Court award punitive or exemplary damages, to the extent permitted by law;

5. That the Court award to Business Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

6. That the Court award pre- and post-judgment interest at the maximum legal rate; and

7. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Business Plaintiffs demand a jury trial on all claims so triable.

Dated: May 14, 2018 Respectfully submitted,

/s/ Amy E. Keller
Amy E. Keller
Adam J. Levitt
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dlcfirm.com
alevitt@dlcfirm.com

/s/ Kenneth S. Canfield
Kenneth S. Canfield
Georgia Bar No. 107744
DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree Street, N.E.
Suite 1600
Atlanta, Georgia 30309
Tel. 404.881.8900
kcanfield@dsckd.com

/s/ Norman E. Siegel
Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel. 816.714.7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com

Consumer Plaintiffs' Co-Lead Counsel

Roy E. Barnes
John R. Bevis
J. Cameron Tribble
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, Georgia 30060
Tel. 770.227.6375
roy@barneslawgroup.com
bevis@barneslawgroup.com
ctribble@barneslawgroup.com

David J. Worley
EVANGELISTA WORLEY LLC
8100A Roswell Road Suite 100
Atlanta, Georgia 30350
Tel. 404.205.8400
david@ewlawllc.com

Consumer Plaintiffs' Co-Liaison Counsel

Rodney K. Strong
GRIFFIN & STRONG P.C.
235 Peachtree Street NE, Suite 400
Atlanta, Georgia 30303
Tel. 404.584.9777
rodney@gspclaw.com

Consumer Plaintiffs' State Court Coordinating Counsel

Andrew N. Friedman
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW
Suite 500
Washington, D.C. 20005
Tel. 202.408.4600
afriedman@cohenmilstein.com

Eric H. Gibbs
David M. Berger
GIRARD GIBBS LLP
505 14th Street
Suite 1110
Oakland, California 94612
Tel. 510.350.9700
ehg@classlawgroup.com

James Pizzirusso
HAUSFELD LLP
1700 K Street NW Suite 650
Washington, D.C. 20006
Tel. 202.540.7200
jpizzirusso@hausfeld.com

Ariana J. Tadler
MILBERG TADLER PHILLIPS GROSSMAN LLP
One Penn Plaza
19th Floor
New York, New York 10119
Tel. 212.594.5300
atadler@milberg.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel. 813.223.5505
jyanchunis@forthepeople.com

William H. Murphy III
MURPHY, FALCON & MURPHY
1 South Street, 23rd Floor
Baltimore, Maryland 21224
Tel. 410.539.6500
hassan.murphy@murphyfalcon.com

Jason R. Doss
THE DOSS FIRM, LLC
36 Trammell Street, Suite 101
Marietta, Georgia 30064
Tel. 770.578.1314
jasondoss@dossfirm.com

Consumer Plaintiffs' Steering Committee

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was filed with this Court via its CM/ECF service, which will send notification of such filing to all counsel of record this 14th day of May 2018.

/s/ Amy E. Keller